ICT Acceptable Use Policy

September 2016

Version No: 0.2
Issue Date: 21/09/2015

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Author
0.1	24/09/2015	New policy rewritten to reflect current changes in technology	Claire Brookes-Daniels
0.2	21/09/2016	Annual review – ensuring content is up to date	Paul Ubaka

DOCUMENT APPROVAL

Version	Date Approved	Description of Approval	Approver
0.1	25/09/2015	Approved in principal prior to the next IG Board Meeting	Paul Golland, CIO

DOCUMENT LOCATION

Document Location	File Name
S:\ICT Acceptable Use Policy v0.1	Forestnet

TABLE OF CONTENTS

1 BACKGROUND

ICT has developed significantly in the last decade and LBWF Council is embracing the opportunities offered by ICT for delivering services, enhancing engagement and communicating with staff, residents, the media and the general public.

The new ICT Acceptable Use Policy reflects the growth in the use of mobile information technology, such as smart phones, tablets and other hand held devices and social media sites, such as Facebook, Twitter, blogs, Linkedin, forums and podcasts.

The policy reflects these changes and other changes and clarifies the Council's expected standards of behaviour in relation to staff who use ICT at work or at home and will replace the 2013 policy.

2 INTRODUCTION

Effective use of technology enhances the Council's efficiency and reputation, providing opportunities to communicate internally, with partners and with the public. The use of electronic equipment, technology and information carries certain risks which can affect the Councils in terms of legal liability, reputation and business effectiveness.

To maximise the benefits, manage risks and protect the Council and its employees, this Policy outlines the standards of conduct required of you when using all electronic communications and systems.

3 PURPOSE

The purpose of this policy is to set out individual responsibilities which assist in protecting London Borough of Waltham Forest (the Council) data and Information Communication Technology (ICT Systems).

It provides standards of conduct regarding the acceptable use of Council ICT systems and forms a part of the LBWF ICT Security Policy.

4 SCOPE

This policy applies to all LBWF employees, council members and volunteers **whether or not you are** provided with or use Council IT systems.

Agency staff working in the Council, consultants and contractors will be required to comply with the standards outlined in this policy while they are working for the Council. Any issue of concern or where potential misconduct is identified will be dealt with under their respective organisations' employment policies and/or the contract.

5 OBJECTIVE

- Staff have a better understanding of the standards of behaviour expected of them when using ICT.

- Clarity for managers and staff of acceptable and unacceptable user of ICT resulting in a reduction of incidents of inappropriate use.

- Staff are confident to use ICT to develop and support new ways of delivering services to further the Council's objectives.

6 DEFINITIONS

Electronic equipment and technology includes all computers and telephone equipment including mobile phones, multi-media devices, PC's laptop computers, tablets, faxes, and any other form of electronic equipment. It also applies to any **personal electronic equipment** or technology that an employee uses in the course of their employment. The Council's electronic equipment and technology will be referred to as "Council ICT systems."

Electronic communications include emails, text messages, instant messaging, images, fax messages, phone calls and voice messages, intranet and internet content/message including social media sites.

Social Media includes websites and online tools that allow users to share content, express opinion or interact with each other e.g. Facebook, Twitter, Linkedin, forums, blogs, podcasts and content communities e.g. You Tube, Flickr, Knowledge hub.

Data includes any electronic or paper information stored or processed on Council networks or equipment including documents, pictures, and/or photographs, music and/or video clips.

These definitions are not exhaustive.

7 MONITORING AND REGULATION

The Council will record the use of its systems to measure system security, performance, whether employees are meeting the standards of conduct in this policy and for the prevention and detection of crime.

The Council will log all internet and email activity, and reserves the right to access, retrieve and delete:

- All email, including in draft form, sent and received;
- All private and shared directories;
- All use of intra / internet and other communication facilities using the Council's ICT systems, for example, Twitter, blogs, etc; and
- All software and computer equipment.

Use of the Council's telephone, fax and mobile telephones will also be logged and may be recorded.

The Regulation of Investigatory Powers Act (2000) sets out the circumstances when it is legal for an organisation to monitor and record communications when they enter, or are being sent within, the organisation's ICT systems. These are where:

- The employer reasonably believes that the sender and person intended to receive it have consented to the interception; and / or;
- The employer may monitor without consent in certain circumstances, for example, to prevent crime, protect their business or to comply with financial regulations.

The Act applies to public and private communication networks. It gives the person who sends or receives a communication the right to claim damages against the organisation for the unlawful interception of communications.

The Council does not routinely monitor or access user activity logs. Where access to these logs is required it must be part of a formal disciplinary or monitoring procedure. Access will be co-ordinated through the ICT Security Architect, who will handle all requests in confidence.

8 COMPLIANCE

If you fail to follow the standards of conduct set out in this policy, use of the Council's ICT systems may be withdrawn from you and / or disciplinary action taken against you, up to and including dismissal.

Appendix 1 gives some examples of activity and behaviour which may be considered unacceptable.

9 ROLES, RESPONSIBILITIES AND DUTIES

The Council may be held legally liable for any statements made on contractual arrangements entered into by its employees through electronic means. It also has a responsibility to make sure the information we hold on clients, residents and employees is held confidentially and securely.

This section describes the expected responsibility in relation to Acceptable Use:

Role	Responsibilities
All employees	• Making sure you have read and understood the ICT Acceptable Use Policy; • Meeting the standards of conduct set out in this policy and any associated guidance which is published on ForestNet; • Undertaking any training as directed by your manager to ensure you understand how to use ICT systems correctly, including

	communications and use of language; and • Ensure that any Council ICT equipment that you take outside the workplace including, but not limited to laptops, mobile phones, tablets, are kept securely so that they cannot be used by others and are kept out of sight if unattended. • Reporting to your line manager any content, comment or information relating to the Council which you know or think could be illegal, defamatory or supports corruption or bribery. • Reporting to your line manager any faulty equipment and the loss or theft of any equipment. • Reporting to your line manager any actual or potential breaches of the Council's ICT security and/or loss of confidential data. • Returning any Council ICT equipment to your manager when you leave the Council.
All Managers	• Ensuring that your staff including new recruits to the Council, are inducted in, aware of and understand the Policy associated guidance and the consequences of any breach of the Policy. • Deciding which employees will have access to the Council's electronic equipment, data and information technology, to assist them in carrying out their duties and responsibilities, and to keep them under review. • Ensuring that employees using ICT to carry out their duties have appropriate training in the use of the Council's ICT systems. This includes appropriate training on the Data Protection and Information Sharing. • Taking action at the earliest signs of a breach of the Policy and/or data Protection regulations. • Taking action when any breach or potential breach of security or confidentiality or loss or damage to ICT equipment is reported to you. • Authorising employees' use of personal electronic equipment and technology for work purposes when it is required to carry out their duties effectively. • Authorising employees' remote access to Councils networks and communications (e.g. e-mail/webmail) to allow for working from home. • Ensuring that all personal information is processed in accordance with data protection legislation. • Supporting the monitoring arrangements on the use of the Council's ICT systems. • Ensuring that employees are removed from the Councils' ICT systems and any Council equipment is returned to ICT when employees leave the Council.
LBWF ICT	• Defining the Council's ICT Strategy, approving ICT systems, equipment, networks and websites and making them available to staff to use during the course of employment.

	• Setting up, maintaining and managing a security configuration (set up) for Council ICT equipment.

10 STANDARDS OF CONDUCT

10.1 General Use of Council ICT Systems

Any information created or held on Council ICT systems will be considered to be owned by the Council. You should not consider any electronic information to be private if it has been created or stored on Council ICT systems. This includes email and internet communications.

You must make sure you communicate in a way that supports the Council's policies including those on equalities. You should therefore make sure that you **do not** send /upload/post information on-line which:

- Damages the Council's reputation or undermines public confidence in the Council;
- Supports political activity (other than any required in your role);
- Includes libellous or defamatory material about an individual, organisation or body; or
- Harasses, bullies or stalks another person.

You should not use personal electronic equipment and technology for work unless you have permission for your manager. If permission has been given the standards of conduct in this policy will apply to your personal equipment when using them for work purposes.

If you make an electronic comment on the internet (blogs, social media, twitter etc.) on a personal basis you must be aware that, as an employee of the Council you are expected to comply with the Standards of conduct and behaviour policy, the Employee Code of Conduct and the Disciplinary Code.

You must not claim to represent the views of the Council unless you have permission to do so as part of your job. Similarly, you must not try and pass off your own comments or views as being from someone else by, for example, falsifying your email address or using someone else's.

You must not use social media, the internet, media, or social media sites to make complaints about your employment. If you want to make a complaint about any aspect of your employment with the Council you must use the appropriate employment procedure (e.g. Grievance, Fair Treatment at Work etc.)

Data which involves images of people is covered by strict rules which prevent the use of sensitive data on children and vulnerable adults. You should therefore check any available guidance relating to your role and work area before using this type of data.

You must ensure that any data stored and/or processed using the Council ICT system complies with the laws on data protection and copyright, is shared only with the intended

recipient(s) and only when permission has been given or the information is already widely in the public domain.

You must not email, upload or post confidential or sensitive data relating to individuals, partner organisations or any aspect of the Council's business on the internet, or remove it from Council property without permission from your manager.

You must maintain security information by, for example, logging off. Accidental disclosure of personal information can occur if unattended computers are left logged onto systems or a computer is not shredded prior to disposal. You should not leave any mobile equipment unattended unless absolutely necessary and if you do so you must ensure that it is secure and protected from risk of theft or use by others.

You must keep your password(s) confidential (do not share them with anyone) and comply with password security arrangements.

You must not process or store Council information on non-Council equipment unless you have permission from your manager or you are using an ICT Service which has been approved by the ICT Technical Design Authority (TDA).

You must not download or install any software, hardware or other devices to Council ICT systems or equipment unless you have permission from your manager. This includes 'free' software, screensavers and games.

It is a criminal offence to use a mobile device whilst driving and conviction will attract a fixed penalty notice and a license endorsement. If, in connection with your employment, you are caught driving whilst using a mobile phone or device you may be subject to disciplinary action and will be responsible for the payment of any fines/penalties imposed on you.

10.2 Standards of Conduct – Personal Use of Council ICT Systems

Personal use of Council ICT Systems will be permitted on a limited basis, subject to the standards of conduct outlined in this policy. The Council reserves the right to restrict personal use of its ICT systems.

Personal use of the Council email and telephones: It is accepted that you may occasionally need to use Council systems to make an important call or to send an important email during working time but these should be kept to a minimum. Personal text/calls/emails must, wherever possible be conducted in your own time. (This also applies to personal calls/emails/texts using your own personal equipment during working time).

Personal calls/text messages on Council-owned telephones: The Council can charge you for the cost of these. The Council reserves the right to charge for personal use of any ICT systems provided for business use.

Personal use of the internet: This is permitted in your own time i.e. outside normal working hours or any additional hours approved by your line manager. If you require the use of the internet for personal use during working time you must get consent from your manager.

Personal use of social media sites: The Council will determine which social media sites may be accessed by staff for personal use. Some sites may not be accessed on ICT systems and these will appear 'blocked' on your screen.

Any personal use of Council ICT systems must not expose the Council's security, systems or data to risk. You must not:

- Circulate non-business emails;
- Allow non-Council employees (including family members) to use Council equipment; or
- Attach any personal equipment to Council ICT systems without the approval of the ICT Security Architect.

You must not knowingly access or try to access inappropriate internet sites, materials or downloads. Pornographic, illegal or other sites which would breach the Council's Employee Code of Conduct, Disciplinary Code or equality standards, must not be accessed from Councils ICT systems or from personal equipment when it is used for work purposes or in work time.

10.3 Standards of Conduct – Use of Social Media

Your manager will decide if you need access to social media sites to carry out your duties at work and you will be given access to them. In order to access them you will have a personal social media account. When you are using social media you must behave in accordance with the standards set out in this Policy.

When using social media sites you must not publish or post any information that you have received or have access to as a result of your employment unless you have permission, as this is confidential to your work.

You must not use social media sites in any way that may undermine public confidence in the Council, bring the Council into disrepute, or would be discriminatory or defamatory e.g. publish or post any information including comments, jokes, illegal or prohibited images or other materials which would put the Council at risk of legal action being taken against it.

You should avoid informal personal contact with pupils or service users you work with directly, or their carers, through social media sites (e.g. do not add them as a 'friend'. to 'follow' them or link with them), using your own personal electronic equipment (e.g. email, texts, calls).

You must not use social media to harass, bully or stalk, or behave in any other way that could damage your working relationships with your colleagues, members of the public or

elected members.

11 DISSEMINATION AND IMPLEMENTATION

This policy will be made available to all relevant stakeholders via the LBWF intranet site. Additionally, they will be made aware via email and this policy will be included for reference where necessary.

This policy will be supported by additional policies and procedures to support implementation.

12 REVIEW OF THE POLICY

This policy will be reviewed on an annual basis, and in accordance with the following on an as-and-when required basis:

- In Legislative or case law changes;
- Changes or release of good practice or statutory guidance;
- Identified deficiencies, risk or following significant incidents reported;
- Changes to organisational infrastructure.

13 APPENDIX 1

Unacceptable Use of Council ICT Systems

This appendix gives some examples of activity or behaviour which may be considered to be unacceptable use of the Council's ICT systems. The behaviours and activities described below may affect whether you can continue your job and may also result in disciplinary action being taken against you which can include dismissal from your post.

In certain circumstances failure to follow the standards of conduct may also be unlawful, and your activities may be reported to the police and may result in criminal proceedings against you.

Certain jobs are also governed by external registration requirements of professional standards of conduct. The Council is required to notify certain external registration bodies of any misconduct by and / or disciplinary action taken against staff.

Examples of unacceptable activity and behaviour are below:

13.1 Personal Behaviour

- Using work time to send personal emails, telephone calls or text messages over and above the limited use described in this policy.
- Accessing the internet for personal use during working time.
- Circulating non-business emails.

- Allowing people not employed by the Council (including family members) to use Council equipment.
- Harassing, bullying or stalking another person online.
- Sending any material that is discriminatory or damaging to others such as jokes, comments, pictures or other material.
- Knowingly accessing or trying to access inappropriate internet sites, materials or downloads such as pornographic, illegal or other sites. This applies to Council ICT systems and to your own personal electronic equipment and technology when it is used for work purposes or in working time.
- Sending, uploading, posting and publishing online any information or comment about an XXXX company or organisation which is defamatory or libellous.
- Connecting or linking with service users, their carers or pupils that you work with on social media (such as Facebook, LinkedIn, etc).
- Using a mobile device while driving.

13.2 Security

- Sharing your password(s) or failing to comply with other security arrangements.
- Attaching any personal equipment to the Council ICT systems without the approval of the ICT Technical Design Authority (TDA).
- Using your own personal electronic and technological equipment for work without permission.
- Accessing personal webmail accounts, such as Hotmail, on Council's ICT systems. (These sites are not protected by the Council's security systems and accessing them will put the Council's ICT systems at risk of virus or malware attacks).
- Downloading or installing software, hardware, etc. onto the Council's ICT systems without permission.
- Trying to access a part of the Council's ICT systems which you do not have permission to access or deliberately trying to damage or disrupt them.

13.2 Public Activity

- Making public information that you have received or have access to as part of your employment – this is confidential to the Council.
- Giving information to the media if you are not authorised to do so by your manager.
- Posting (publishing) any information on the internet or social media sites as a representative of the Council unless you have permission from the Council Web Team.
- Claiming that you represent the views of the Council without permission.
- Making public any information which may undermine confidence in the Council or damage the Council's reputation.

- Carrying out internet-based searches on applicants or candidates for jobs in the Council, unless you are asked to by the candidate.
- Making a complaint about your employment publicly through internet, intranet, media or social media sites.

This is not an exhaustive list.