# Conditions of Acceptable Use

# Version Control Sheet

| | |
|---|---|
| **Title:** | Conditions of Acceptable Use |
| **Purpose:** | To advise staff of the Council's responsibilities for Acceptable Use |
| **Owner:**<br>**Author:** | Data Protection Advisor<br>lhenley@thurrock.gov.uk<br>01375 652500 |
| **Approved by:** | |
| **Date:** | March 2019 |
| **Version Number:** | 1.0 |
| **Status:** | Draft |
| **Review Frequency:** | As and when changes take place to Information Governance Legislation. |
| **Next review date:** | As Above |

## 1. Introduction

The Conditions of Acceptable Use document defines acceptable use of Information and Communication Technology within *Brentwood Borough Council* and is in support of the Corporate Information Security Policy.

## 2. Definitions

Information security is the preservation of:

- **Confidentiality**: ensuring that information is accessible only to those authorised to have access;
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods;
- **Availability**: ensuring that authorised users have access to information and associated assets when required.

The Conditions of Acceptable Use and other Information Security policies are underpinned by the Personal Commitment Statement which details a list of specific compliance requirements.

## 3. Scope

This applies to any employee, elected member, agency worker, third party organisation or other authorised personnel

## 4. Authority

This policy is supported by Chief Executive of Brentwood Borough Council

## 5. Objectives

The objective of the Acceptable Use Policy is:

- To protect information and communication technology from unacceptable use.

## 6. Roles and responsibilities

All roles and responsibilities are outlined in the Corporate Information Security Policy.

## 7. Conditions of Acceptable Use

You **must not:**

- Access or attempt to access any computer material, (that is a program or data), that you are not authorised to access.
- Access or attempt to access a computer system with the intent to commit or facilitate the commission of a criminal offence.
- Use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse;
- Attempt to access the PSN other than from IT systems and locations which I have been explicitly authorised to use for this purpose

- Transmit information via the PSN that I know, suspect or have been advised is of a higher level of sensitivity than my PSN domain is designed to carry;
- Transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated;
- Make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received);
- Carry out unauthorised modifications to any computer material.
- Undertake any unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to material of a pornographic, sexual, violent or criminal content, racist, sexist or otherwise discriminatory nature.
- Install software without approval of *ICT Manager a*nd this **must** be for business purposes subject to compliance with license restrictions.
- Send information marked OFFICIAL-SENSITIVE over public networks such as the Internet unless approved encryption has been applied to it
- Send or forward any chain emails (e.g. jokes) except to report them as defined in the Security Incident Reporting and Management Procedures.
- Use Brentwood Borough Council's facilities or Brentwood Borough Council identity for commercial purposes outside of the authority or remit of Brentwood Borough Council or for personal financial gain unless authorised to do so.
- Rely on building controls such as security doors to prevent unauthorised access or use.
- Do anything that would compromise the security of the information as defined in Corporate Information Security Policy
- Attempt to introduce viruses, Trojan horses or any other malware into the system, and must not attempt to disable or bypass anti-virus protection or delay updates provided on your computer.
- Disclose in writing, speech or electronically information held by Brentwood Borough Council unless you are authorised to do so and recipients are authorised to receive it.
- Attempt to disable measures which prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation),
- Attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;
- Remove equipment or information from my employer's premises without appropriate approval;
- Disable anti-virus protection provided at my computer

You **must:**

- Lock equipment or log out of the workstation when leaving it unattended even for a short time.

- You are responsible for helping to maintain the security of information held by Brentwood Borough Council.
- Protect such credentials at least to the same level of Protective Marking as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises);
- Seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted;
- Take appropriate steps to secure the equipment and information to which you have access. When your equipment or information is unattended,
- Report actual or suspected information security incidents, events or weaknesses to the Data Protection Team or ICT Manager
- Report any detected viruses to ICT Manager immediately and **ONLY** to the *ICT Manager.*
- When printers, photocopiers or faxes are used for protected, restricted or sensitive information they must be attended by an appropriate person if the printer doesn't support printer mailboxes.
- Security of electronic information is achieved through the use of logins and passwords. You must log in using your own login name and a secure password known only to you.
- Report all faults to *ICT Services.*
- You are provided with facilities for business use only; limited personal use is acceptable if it meets the criteria defined in other policies.
- If you are a manager, you must also ensure that users you are responsible for are aware of, and comply with, this policy.
- If you are a user of N3, you must also comply with the NHS Statement of Compliance requirements.
- If you are a user of N3, you must also comply with the NHS Statement of Compliance for 3rd Parties.
- If you access any systems such as NHS or Government, through other secure networks such as EssExtranet you must only use those systems for the purpose for which they have been authorised, and they must not establish, or attempt to establish an onward connection once they have gained access to the end system.
- Make yourself aware of your organisation's security policies and procedures together with any additional requirements which may be associated with connection to secure networks such as PSN.
- Protect any material, whatever the sensitivity or protective marking, sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material
- Use the provided facilities economically.

- Take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief);
- Comply with the Data Protection Act and any other legal, statutory or contractual obligations that my employer informs me are relevant
- Inform my manager prior to my departure from my employment of any important information held in my account.

You **should not**:
Access mobile services from outside the UK using corporate devices or your own device to access Brentwood Council System and Data, unless you have been made aware of the risks of using mobile technology abroad.

## Acceptable Use of email

You **must not:**

- Use e-mail for offensive or unlawful activities, commercial purposes or personal financial gain.
- Access or disclose other people's e-mail without their permission.
- Subscribe to services using Brentwood Borough Councils e-mail address unless representing Brentwood Borough Council.
- Send unsolicited, irrelevant or inappropriate e-mail to multiple newsgroups or mailing lists.
- Forward or disclose any sensitive or protectively marked material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel
- Use your GCSX email address as a sender field when emailing content from the Internet to GCSX
- Not knowingly disrupt Brentwood Borough Council's e-mail service or send emails from another users address unless the email identifies the sender i.e. 'on behalf of'.
- Auto-forward email from my PSN account to any non-PSN email account;
- Refer to Email Policy for additional requirements.

You **must:**

- Always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain
- Disclose information received via the PSN only on a „need to know" basis
- Protect the confidentiality of e-mail you view inadvertently.
- Follow Brentwood Borough Council procedures for authorisation and notification if accessing someone else's e-mail.
- Comply with Brentwood Borough Council policies and any UK law that applies to e-mail.
- Use personal and professional courtesy and consideration when using e-mail.

- Add security labels to each email that carries a protective marking of OFFICIAL-SENSITIVE

You **should not:**

- Rely exclusively on e-mail to archive or retain records.
- Access personal e-mail accounts directly or via the web.
- Send Encrypted files via email unless implementing a business requirement such as protecting personal sensitive information

You **should:**

- Make appropriate arrangements to make your e-mail available to ensure service continuity during any absence.
- Check with the sender if not sure about the authenticity of a message.
- Regularly check your e-mail inbox for new messages.
- Take care when you use the Reply to All function as this may be inappropriate.

## Acceptable Use of the internet

You **must not:**

- Visit web sites that contain inappropriate material. These include but are not limited to pornography, extremist or racist organisations, dating web sites and chat rooms.
- Join forums or other forms of electronic notice board in the name of Brentwood Borough Council other than for legitimate Brentwood Borough Council use. Where passwords are required for forums or any other web or e-mail access outside Brentwood Borough Council *,* different passwords should be used to those used for internal access.
- Publish a web site or anything on a web site that could bring Brentwood Borough Council into disrepute.
- Use any sort of instant messaging software or peer-to-peer software for personal or professional reasons without prior consent from the appropriate manager at Brentwood Borough Council.
- Download software without prior consent from the *ICT Manager* at Brentwood Borough Council. Software includes but is not limited to screensavers, device drivers, shareware, browser add-ins, software patches, add-ons and updates. All software installations must comply with license agreements.
- Commit Brentwood Borough Council to any agreements with third parties over the Internet without prior consent from the appropriate manager.
- Knowingly interfere with other people's use of the internet.
- Unreasonably offend any colleague, or promote/engage in discriminatory behaviour in the workplace.

You **must:**

- Use personal and professional courtesy and consideration when using the internet.

## Acceptable Use of Removable Media

You **must:**

- .
- Follow the Data Security and Encryption Policy.

## Acceptable Use of Authentication

You **must not**:

- Attempt to bypass or disable any security controls.
- Disclose your password to anyone other than for the purposes of placing a secured copy in a secure location at my employer's premises. You are accountable for any action taken using your login and password. If you are asked to log into a computer and allow support staff to access the network, you should note the date and time in case of later query.
- Ask anyone else for their password.
- Tell the system to store passwords so that it can access them without typing them in. Information security relies on the proper use of passwords.
- If you suspect that your password is no longer secure, it must be changed immediately and follow the incident reporting procedure if appropriate.

You **must:**

- Maintain a network password which has to be a minimum of 7 characters long and must be a combination of characters and numbers with at least one character in capital.
- If you find it necessary to record a password, for your own benefit, best efforts must be taken ensure that it is not accessible to anyone else.

You **should:**

- Change Passwords when a breach of security occurs or is suspected.

## Acceptable Use of your own device

You **must:**

- Accept that security management software will be installed on your device prior to it being used for corporate or business use
- Accept that you are personally liable for the device and carrier (service provider) costs.
- Accept all terms and conditions in this policy to be allowed access to Brentwood Borough Council services
- Accept that, when connecting the personal mobile device to Brentwood Borough Council resources, the Brentwood Borough Council security policy will be enforced

on the device. The security policy implemented may include, but is not limited to, areas such as passcode, passcode timeout, passcode complexity and encryption.
- Accept that Brentwood Borough Council data and/or corporate applications on your device may be remotely wiped if you lose it, you terminate employment, IT detects or are notified of a data / policy breach or virus or if you incorrectly type your password an unacceptable number of times in line with Brentwood Borough Council IS policy
- Accept that your Brentwood Borough Council data area will lock after a period of inactivity, in line with Brentwood Borough Council policy, requiring re-entry of your password.
- Accept that Brentwood Borough Council reserve the right to disable or disconnect some or all corporate services without prior notification.
- Accept and acknowledge that you must assume full liability for the use of your device in connection with Brentwood Borough Council business. Potential risks are; the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which have the potential to render a device inoperable.
- Accept that if you leave "data roaming" on whilst abroad, you will not be compensated for the incurred cost.
- Report the loss of personal devices to ICT Services at the earliest opportunity.
- Comply with Brentwood Borough Council policies such as Conditions of Acceptable Use, Code of Conduct, Corporate Information Security and Relevant Health and Safety policies when using your device for business purposes.
- Notify the ICT Services in advance, if you intend to change the device.

You **Must** not:
- Use your device in ways not designed or intended by the manufacturer. This includes, but is not limited to, "jailbreaking" or "rooting" your device.
- Expect technical or user support for personal devices other than corporate apps and data
- Allow non-corporate users to have access to the Brentwood Borough Council data.

You **should**:
- Upgrade and have patches applied to your mobile device as soon as possible in line with manufacturer's recommendations.
- Be aware that your device may allow for only the remote wipe of Brentwood Borough Council data. This means your personal data is still vulnerable and it is recommended you set a device password or take additional security precautions as well.
- Regularly back up your device

## *8 Brentwood Borough Council* specific

Personal use **must not:**

- Interfere with the performance of your duties.
- Make use of information available to you that is not available to the public.
- Result in any additional cost to Brentwood Borough Council.
- Reflect adversely on the reputation of the Brentwood Borough Council.

Personal use **must:**
Be in accordance with the Corporate Information Security Policy, standards and procedures. If personal use is abused, facilities maybe withdrawn

You **must not:**

- Under any circumstances use personal credit/debit cards over the Internet, bid on online auctions or use online banking for personal usage from Brentwood Borough Council computer equipment
- Let personal use of e-mail interfere with your employment or other obligations to Brentwood Borough Council.

You **must:**

- Only use the internet for personal purposes in your own time (i.e. before or after work, or during your lunch break).
- Ensure that data stored on a local workstation is backed up regularly
- Personal use **must** be in accordance with the Information Security Policy and supporting standards and procedures.
- Personal use **must not** interfere with the performance of your duties.
- Personal use **mus**t **not** result in any additional cost to Brentwood Borough Council.
- Personal use **must not** reflect adversely on the reputation of the Brentwood Borough Council.
- If personal use is abused, facilities maybe withdrawn.
- You **must** only use the internet for personal purposes in your own time (i.e. before or after work, or during your lunch break) or as approved by your Line Manger.
- You **must not** let personal use of e-mail interfere with your employment or other obligations to Brentwood Borough Council.
- You **must** ensure that data stored on a local workstation is backed up regularly.
- Removable media such as USB flash drives **must** be encrypted and **must** of an approved model.
- The use of removable media will be monitored and PC's will be prevented from using it unless a valid business case is presented to the ICT Manager**.**
- All Council laptops **must** have the hard disk drives encrypted.
- When transferring data to third parties you **must** ensure the appropriate measures are taken to protect that data. This may required that data is encrypted to an approved standard before it leaves the Council.
- Infringement of the above statements may result in disciplinary action

## 9. Personal Commitment Statement

$u1nlb4ne

## Introduction

This personal commitment statement is in support of *Brentwood Borough Council* Corporate Information Security Policy.

## Scope

A personal commitment statement **must** be in place for every user of the Brentwood Borough Council information and resources.

*"I understand and agree to comply with the security rules of* **Brentwood Borough Council** *which include:*

*For the avoidance of doubt, the security rules relating to secure e-mail and IT systems usage include:*

*I*

- acknowledge that my use of the PSN may be monitored and/or recorded for lawful purposes;
- agree to be responsible for any use by me of the PSN using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address;
- will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse;
- will protect such credentials at least to the same level of Protective Marking as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises);
- will not attempt to access any computer system that I have not been given explicit permission to access;
- will not attempt to access the PSN other than from IT systems and locations which I have been explicitly authorised to use for this purpose
- will not transmit information via the PSN that I know, suspect or have been advised is of a higher level of sensitivity than my PSN domain is designed to carry;
- will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated;
- will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received);
- will protect any material, whatever the sensitivity or protective marking, sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material;
- will not send information marked OFFICIAL-SENSITIVE over public networks such as the Internet unless approved encryption has been applied to it;
- will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain;
- will not auto-forward email from my PSN account to any non-PSN email account;
- will disclose information received via the PSN only on a „need to know" basis;

- will not forward or disclose any sensitive or protectively marked material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel;
- will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted;
- will securely store or destroy any printed material in accordance with the Brentwood Borough Council Documentation Retention Policy;
- will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the PSN (this might be by closing the e-mail program, logging-off from the computer, activating a password-protected screensaver, etc., so as to require a user logon for activation); and
- will not leave information unattended in such a state as to risk unauthorised disclosure of information
- Where my organisation has implemented other measures to prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection;
- will make myself familiar with the security policies, procedures and any special instructions that relate to the PSN;
- will inform ICT Manager immediately if I detect, suspect or witness an information security incident or problem that may be a breach of security;
- will not knowingly attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;
- will not remove equipment or information from my employer's premises without appropriate approval;
- will take precautions to protect all information and computer media and portable computers when carrying them outside my organisations' premises (e.g. not leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief);
- will not knowingly introduce viruses, Trojan horses or other malware into the system or PSN;
- will not disable anti-virus protection or delay updates provided at my computer;
- will comply with the Data Protection Act and any other legal, statutory or contractual obligations that my employer informs me are relevant; and
- If I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account."

I am aware of the disciplinary procedures of Brentwood Borough Council in the event of non-compliance with this commitment

*When I use my own device;*
*"I*

$u1nlb4ne

- will make my device available for security management software to be installed
- will be personally liable for the device and carrier (service provider) costs.
- accept all terms and conditions in the BYOD policy to be allowed access to Brentwood Borough Council services
- accept that, when connecting the personal mobile device to Brentwood Borough Council resources, the Brentwood Borough Council security policy will be enforced on the device. The security policy implemented may include, but is not limited to, areas such as passcode, passcode timeout, passcode complexity and encryption.
- accept that Brentwood Borough Council data and/or corporate applications on my device may be remotely wiped if I lose it, if I terminate employment, if IT detects or are notified of a data / policy breach or virus or if I incorrectly type my password an unacceptable number of times in line with Brentwood Borough Council IS policy.
- accept that my Brentwood Borough Council data area will lock after a period of inactivity, in line with Brentwood Borough Council policy, requiring re-entry of my password.
- accept that Brentwood Borough Council reserve the right to disable or disconnect some or all corporate services without prior notification.
- accept and acknowledge that I must assume full liability for the use of my device in connection with Brentwood Borough Council business. Potential risks are; the loss, damage or theft of hardware, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which have the potential to render a device inoperable.
- accept that Brentwood Borough Council will not be responsible for providing any support in relation to my device
- report the loss of personal devices to ICT Services at the earliest opportunity.
- comply with Brentwood Borough Council policies such as code of conduct Information security mobile phone policy and relevant Health and Safety
- notify the ICT Services in advance, if I intend to change the device.
- will not use my device in ways not designed or intended by the manufacturer. This includes, but is not limited to, “jailbreaking” or “rooting” my device.
- will not expect technical or user support for personal devices other than corporate apps and data
- will not allow non-corporate users to have access to the Brentwood Borough Council data.
- will aim to upgrade and have patches applied to my mobile device as soon as possible in line with manufacturer’s recommendations.
- will be aware that my device may allow for only the remote wipe of Brentwood Borough Council data. This means my personal data is still vulnerable and it is recommended I set a device password or take additional security precautions as well.
- will aim to regularly back up my device

Signature……..Date……

Senior Manager Signature……Date……

$u1nlb4ne

Please print

| | |
|---|---|
| **Name** | |
| **Job Title** | |
| **Place of Work** | |

v1.3.2