Acceptable Use of ICT Policy

Author:	**Alison Hughes, Assistant Director – Strategic ICT Partnerships**
Date:	**30 April 2018**
Version:	**10.0**

Document Control

Revision / Review History		
Revision / Review Date	**Reviewer**	**Description of any Revisions**
Version 1		
Version 2 – September 2012		Re-issued
Version 3 – February 2013		Updated to include Guidance for Elected Members.
Version 4		Updates to care of devices, monitoring of activity and classification of use of email.
Version 5		Update to forbidden section in 2.3 and other minor amends.
Version 6		Inclusion of use of tablet devices throughout, update to forbidden section in 2.3, addition to unacceptable section in 2.5.
Version 7		Change of defined term 'Phones' to include pool phones. Change in status of acceptable use of Council phone from Acceptable and Unacceptable to Forbidden.
Version 8		Reviewed for relevance – no changes made.
Version 9	Alison Hughes	2.3 – GCSX Staff – Please note remote access from devices using unsupported platforms is now forbidden. 2.5 – GCSX Users – Please note. 2.6 – Changes to "what equipment and support is provided". Paragraph 3 updated. Paragraph 5 deleted. Page 2.6, Page 14 – Confidentiality – Last line references use of Egress. 2.6, Page 14 – Use of Email "Avoid large attachments".
Version 10	Andrew Roberts	2.2 Sharing personal data 2.3Reference to confidential waste policy 2.5 Page 12 Reference to prohibition to send personal data via SMS/SMS 2.6 Point 4 – Inclusion of the word "Personal" 2.6 Page 13 – Reference to GDPR included and amended DPO details 2.6 – Page 14 – Confidentiality – Also applies to staff 3.0 Page 15 – Adherence to GDPR bullet

What has Changed?

Updates around implementation of GDPR and use of personal data.

Contents

Further documentation referred to here can be found on the

IT Security Policy Page

1.0 Introduction

Why do we have this Policy? We want you to use our ICT with Confidence

Wigan Council is a Digital Council and encourages the wide scale use of its ICT Systems and Services for communicating with customers, clients and others for business related purposes.

The aim of this code of practice is to clearly outline what Wigan Council considers to be acceptable, unacceptable and forbidden use of its ICT and to protect the Councils information from loss, unauthorised access and cyber-crime.

This code of practice for ICT refers to system applications, internet, email, mobile devices (including telephones, cameras etc), telephone landlines, personal computers, laptops, tablets and servers.

The aim is not to impose unnecessary restrictions, but rather to ensure that you and managers are fully aware of the rules surrounding the use of ICT and to enable them to make safe and appropriate use of it. This code also protects the Councils data from cyber-crime and unlawful disclosure.

Who does this code apply to?

Everybody who is an authorised user of the Council's systems or ICT services (including users accessing remotely).

This includes: Council employees, partner organisation employees (utilising the Council network), Elected Members, agents and contractors who directly or indirectly support or have access to the Councils ICT systems.

Wigan Council ICT		
Council's Responsibilities	**Your Responsibilities**	**Managers Responsibilities**
Keep Systems and Data about citizens secure.	**Use Safely, Securely and efficiently in a professional manner, being vigilant about cyber threats.**	**Effectively manage access to systems.**
Monitor Usage and maintain accurate digital records.	**Take care of devices – Protect from damage, loss and theft.**	**Share this code with staff on induction, during team briefings and as part of appraisal.**
Comply with the law.	**Understand your responsibilities under data protection.**	**Read Policy and encourage staff ICT development.**

1.1 Definitions in this Policy

This policy defines the Council’s view on what it considers to be acceptable, unacceptable and expressly forbidden use of ICT.

All employees and Elected Members must comply with the Council’s Code of Conduct for Employees and Elected Members and with the law in their use of the Council’s ICT.

Examples of acceptable, unacceptable and forbidden include but are not limited to the examples quoted in this policy.

The definitions are outlined below:

✓ Acceptable

The activities listed as acceptable define the degree of flexibility that Wigan Council allows to all authorised users of ICT. The Council wants people to feel comfortable using new technologies and to seek opportunities to work in a more digital way.

✗ Unacceptable

People carrying out activities in this category will be regarded as in breach of the Code of Conduct Employees and Elected Members and this may result in action under the Council’s disciplinary procedure. Unacceptable behaviour could also be classified as gross misconduct if significant enough, e.g. long periods, persistent misuse, several unacceptable activities taking place. This could ultimately lead to dismissal from employment.

🚫 Forbidden

People carrying out activities in this category will be regarded as in breach of the Code of Conduct for Employees and Members, and this will be subject to action under the Council’s disciplinary procedure and may constitute gross misconduct where appropriate. This could ultimately lead to dismissal from employment. Users may also be subject to civil criminal proceedings.

As a general guide, if there is any doubt about what is meant by acceptable, unacceptable or forbidden use for ICT, you should seek advice from your Management, the ICT Helpdesk, Internal Audit or the Casework Team, People Services.

Contact Details for the ICT Helpdesk.
Telephone Number: 4142 (01942 404142).
ICT Self Service Log in: https://itportal.agisw.co.uk

2.0 Acceptable Use of Wigan Council's ICT Systems and Services

The following sections clearly outline what the Council considers to be acceptable, unacceptable, and forbidden use of the Council's ICT under the headings internet, email, PCs, laptop, tablets and servers, user accounts and passwords and telephone (mobile and landline) use.

It is important to note that examples of acceptable, unacceptable and forbidden activities include, but are not limited to those quoted in the Acceptable Use Policy.

2.1 Use of Internet Services

The Council's position of acceptable, unacceptable ad forbidden use of the Internet is defined below:

✓ **Acceptable**

- Accessing business related web sites in relation to your job;
- Accessing non-business related web sites outside of your working hours;
- Any personal use must not include any activity outlined in the 'unacceptable' and 'forbidden' sections below.

✗ **Unacceptable**

- Providing your work email address as contact details to sites you have accessed for non-business purposes. **Why?** This poses a potential security risk to the Council's network by encouraging spam emails or chain emails;
- Spending any periods of the time you are booked in as working looking at non-business related Internet sites e.g. Facebook. **Why?** This is not good use of your time;
- Downloading any copyright material without the owner's permission. **Why?** This is against the law.

🚫 **Forbidden**

- Use of unsecured Wi-Fi connections such as, but not limited to, coffee shops, stores, hotels or restaurants. Please note: GCSX mail users will only be permitted to connect via either Wigan corporate Wi-Fi, home Wi-Fi or corporately provided 3G/4G. **Why?** Risk of cyber-criminals hacking your work credentials;
- Using web based email for example Facebook emails, Google mail etc from your work equipment. **Why?** This is insecure.
- Spending any excessive periods of the working day looking at non-business related internet sites. **Why?** Not good use of resources.
- Downloading software used for hacking or cracking passwords without prior

consultation with ICT. **Why?** This is against the law.

- Making repeated attempts to access web sites that, because of their inappropriate content, have been automatically blocked by the Council's web filtering software. **Why?** These sites are blocked because they present a security risk.
- Tying up internet resources on non-business related activity, to the detriment of genuine business internet usage. This includes leaving live internet feeds open to collect news or sports results and downloading images, video or audio streams for non-business related purposes. **Why?** Because it affects other people's ability to work.
- Accessing sites containing pornographic, offensive, racist or obscene material that may cause offence to others. **Why?** Inappropriate;
- Using someone else's personal account and password to access the internet. **Why?** This is our audit trail for people and you compromise this.
- Attempting to circumvent / avoid any Wigan Council security features. **Why?** Because it is there for good reasons.

**** It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users.**

2.2 Use of Email Services

The Council's position on acceptable, unacceptable and forbidden use of email is defined below:

✓ **Acceptable**

- Communication in connection with Wigan Council's business;
- Management access to read employees/users mail boxes where there is a legitimate need, authorised by the relevant Head of Service, to do so (e.g. if a person is absent and an important email is expected). This may require the Council to access personal communications to you;
- Limited use of email **internally only** for non-business purposes **and outside of your working hours** but remember this can be viewed.

✗ **Unacceptable**

- Customising emails such as using non-corporate backgrounds, logos or signatures;
- Forwarding chain emails or similar;
- Sending work related information to and from your personal email address;
- Sending business related email directly to large distribution groups (300+), without approval from the Assistant Director Strategic ICT Partnerships.

🚫 **Forbidden**

- **Sharing personal and/or sensitive data without verifying that the Council has the legal powers or explicit consent to do so.**
- Sending messages or files that contain discriminatory, abusive, racist, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content;
- Supplying your work email address for non-business related activities, for example Facebook / Internet Banking / Ebay / Argos etc.
- Sending personal or sensitive business material to employees personal email accounts, or to unauthorised internal or external recipients;
- Excessive use of email internally for personal non business purposes;
- Sending emails from another user account **unless specific approval or permission is obtained, which would be granted for example for specific shared mailbox management;**
- Excessive use of Council email **externally** for non-business purposes;
- Emailing confidential, sensitive or personally identifiable information to other people (internal or external) without ensuring that this data is appropriately secured;
- Sending files with non-business related attachments (e.g. compressed files, executable code, video streams, audio streams or graphical images) to internal or external parties;
- Using web based mail services such as Facebook mail, Google mail etc

**** It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users.**

Note

Unsolicited receipt of discriminatory, abusive, pornographic, obscene, illegal, offensive or defamatory email is clearly not a disciplinary offence, although anyone who receives use material should inform their manager, who should seek appropriate advice from the ICT Helpdesk on extension 4142 (01942 404142).

If anybody receives offensive or pornographic material from a known sender, whether they are themselves offended by it or not, they should immediately and politely make the sender aware that they do not wish to receive any similar material and inform their manager. If the material comes from an unknown source, the message must be deleted immediately without a message being sent back to the originator.

2.3 Use of PCs, Laptops, Tablets, Mobile Phones and Servers

Everybody must take appropriate measures to ensure that any devices supplied to them are protected from damage, loss or theft. In the event of a preventable theft or loss, a charge may be applied. The Council's position on acceptable, unacceptable and forbidden use of PC's, laptop, tablets and servers is defined below:

✓ **Acceptable**

- Creating and storing data in connection with Council business in a way which ensures that this data is regularly backed up. **Note:** laptops must be encrypted before business use and handheld devices password protected;
- Loading text, images, video or audio streams in connection with normal business.

Unacceptable

- Loading any unauthorised or untested software, i.e. software not purchased through the formal purchasing process. This includes, for example, software downloaded from Internet web sites, whether freeware or commercially sold;
- Storing Council data on the local drive of your PC/laptop/tablet, which is not subject to back up routines;
- Storing your own personal data on any Council device including a memory stick, mobile phone, a Council PC, laptop, tablet or server, e.g. music files, films, games, video clips, images;
- Leaving your PC/Laptop/Tablet/Mobile phone unattended without locking the machine or device for PC's, password enabling (for handheld devices) or logging off.

Forbidden

- Use of unsecured Wi-Fi connections such as, but not limited to, coffee shops, stores, hotels and restaurants. Please note: Staff will only be permitted to connect via either Wigan Corporate WiFi, home WiFi, corporately provided 3G/4G or other Government buildings for meetings;
- Loading files containing pornographic, offensive or obscene content, whether in text, image, video or audio format;
- Use of unencrypted laptops for Council business;
- Storing personal material which is protected by copyright, such as pictures, music, video, games etc, software that has NOT been purchased through formal Wigan Council channels;
- Use of unencrypted non Council issued mobile storage devices to store Council data including Council emails;
- Deliberate, reckless or negligent introduction of a virus in to the Councils ICT;
- Installation and/or use of software with remote control capabilities without ICT Security Management consent;
- Storing Council data that contains confidential, sensitive or personal information on the local drive or a PC/laptop/tablet, or removable media e.g. CD/DVD, pen drive etc;
- Storing Council data on any cloud based storage facility e.g. iCloud/OneDrive/Dropbox etc unless authorised by the Partnership SIRO;
- Staff should not connect remotely from devices which are running unsupported platforms – Windows XP for example;
- Printing off any personally identifiable or sensitive information from Council

systems and sharing this with individuals who do not have the right to access this information;

- Not disposing of or storing paper documents containing personally identifiable or sensitive information in a safe, confidential way. (See: Disposal of Confidential Waste policy).
- Attempting to access any computer system that you have not been given explicit permission to access.

**** It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users.**

2.4 Use of User Accounts and Passwords

The Councils position on acceptable, unacceptable and forbidden use of the User network and application Accounts and Passwords is defined below:

✓ **Acceptable**

- Using your own, personally assigned user account to carry out your work at Wigan Council;
- Using administrator accounts to carry out your daily tasks in response to specific administrator activities assigned to you by your manager;
- Access to anybody's accounts without the owner's explicit permission. This can only be granted where there is a legitimate business need the approval is required from the Head of Service.

✗ **Unacceptable**

- Requesting the password for a user account personally assigned to another member of staff.

🚫 **Forbidden**

- Writing passwords down and storing with / near your device.
- Sharing a password associated with any user account assigned to you;
- Resetting the password associated with a user account assigned to someone else, without the owners express permission;
- Providing the password for a user account personally assigned to another member of staff;
- Using a user account that has been provided to another member of staff without correct permission but the Head of Service or above;
- Using a session established by another user under their own personal account;
- Using a privileged user account to access data where there is no specific

business reason to do so.

It is the individuals responsibility to ensure their user account and password details are not disclosed. If there is any suspicion that your details are know then change your password. If you suspect your user account details have been used without authorisation notify your manager immediately.

**** It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users.**

2.5 Use of Telephones (mobiles and landlines)

The Councils position on acceptable, unacceptable and forbidden use of telephones is defined below:

It is important to note that it is a managers responsibility to monitor usage of both landline and mobile telephones. Managers have the responsibility to inform the ICT help desk when a mobile phone is no longer required, e.g. a member of staff has left and the phone is not being passed on, so that the contract can be cancelled.

For the purpose of this policy the term ‘Phones’ refers to Council landlines and mobile telephony devices, including pool phones.

✓ **Acceptable**

- Use of Wigan Council Phones in connection with normal business;
- Use of personal mobile phones for short conversations in work subject to service requirements which may prohibit this (e.g. drivers, people working on public counters).

✗ **Unacceptable**

- Allowing use of Council Phones by an unauthorised person/s;
- Excessive use of personal mobile phones during working hours to make calls, access the internet or send text messages;
- Incurring international roaming costs unless pre-authorised by your manager (or Democratic Services Manager in case of Members).

🚫 **Forbidden**

- Use of unsecured Wi-Fi connections such as, but not limited to, coffee shops, stores, hotels and restaurants. Please note GCSX mail users will only be permitted to connect via either Wigan corporate WiFi, home WiFi, corporately provided 3G/4G or other Government buildings for meetings;
- Use of Council phones for personal calls (this includes the use of SMS text messages) except in an emergency. Your manager must be informed of any

emergency use. Personal use will be monitored and any misuse will result in the facility being withdrawn and disciplinary action being taken;

- Use of phones in a manner that could bring Wigan Council into disrepute;
- Sending SMS or MMS messages that contain discriminatory, abusive, racist, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content;
- Sending personal and/or sensitive data using SMS or MMS messages without verifying that the Council has the legal powers or explicit consent to do so.
- Use of Wigan Council number to promote any external private business;
- Use of Wigan Council phones to contact premium rate numbers.

**** It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users.**

2.6 Guidance for Members on the use of IT Equipment

Why is IT important?

The Councils position on acceptable, unacceptable and forbidden use of telephones is defined below:

The use of ICT is now seen by the Council as a vital pre-requisite for any Councillor to be able to carry out their role effectively. Councillors are increasingly finding that this is how members of the public want to engage with their local Councillors in terms of using ICT equipment and resources for Council purposes.

The Council recognised that many Councillors are very busy people and that a Councillors role is time-consuming and involves dealing with a large amount of information and correspondence, much of which is increasingly electronic. Regardless of which of the options below a Councillor may choose to have, the Council is committed to ensuring that you are provided with a high quality solution that meets your needs. The Council is committed to giving you any support you need to use IT effectively.

Shortly after induction, all Councillors will be given relevant telephone numbers and email addresses, together with detail on how to access this advice and support. Outside of the provision of equipment and facilities, a range of training for all abilities is available, and this will be discussed with Councillors on an individual basis,

How can I ensure that I protect the information I have access to?

Members are reminded at all times of the need to follow the Members Code of Conduct. In relation to ICT, Councillors attention is particularly drawn to their obligations under paragraph 4 in relation to the disclosure of information, and paragraph 5 in relation to general conduct namely.

4. You must not disclose information given to you in confidence by anyone, or information acquired by you which you believe, or ought reasonably to be aware, is of a confidential or personal nature, except where:

- You have the consent of a person authorised to give it;
- You are required by law to do so;
- The disclosure is made to a third party for the purpose of obtaining professional advice provided that the third party agrees not to disclose the information to any other person or the disclosure is:
- Reasonable and in the public interest and
- Made in good faith and in compliance with the reasonable requirement of the authority or
- Prevent another person from gaining access to information to which that person is entitled by law.

5. You must not conduct yourself in a manner which could reasonably be regarded as bringing your office into disrepute.

   Councillors must register with the Information Commissioners Office if they process personal data in electronic format and the processing is in relation to their constituency casework when representing members of their ward (dealing with complaints and issues by the public, diary surgery appointments, write letters as they see fit on behalf of their constituents). This is a requirement of the General Data Protection Regulation, and failure to register when required to do so is a criminal offence.

   The Council's Data Protection Officer will complete the registration process on your behalf. Please phone 01942 827002 internal 2002 or by email gdprqueries@wigan.go.uk.

What equipment and support is provided?

Elected members can choose to be provided with either a mobile phone for phone calls only or a smartphone for phone calls and to receive Council emails. Councillors must ensure that they protect the data held on mobile devices from unauthorised access due to theft or loss, by setting a device password. IT Service Desk can assist with this.

In addition to this, all Councillors can be provided with a tablet device, purchased by the Council. This is the most cost-effective option for the provision of ICT equipment to Councillors and will be provided to Elected Members following completion of mandatory social media training and acceptance by the Member, of the IT Acceptable Use Policy.

The Council will also provide remote access to email and home support and maintenance. In the event of a permanent failure, the equipment will be replaced, unless that failure is due to obvious non-accidental misuse / avoidable loss, in which case the Councillor may be expected to bear the cost of the replacement.

Connection to the Council's network will be via a secure method supported by the Council. This connection will allow you as Councillors full access to the systems and information needed for your role. Log-on passwords for this connection are restricted solely to the Councillor and must not be used by other family members. The Councillor must comply fully with the Council's reasonable requirements regarding confidentiality and emails, which are set out below in.

All Councillors will be required to sign the terms and conditions of usage confirming their understanding and acceptance of these requirements. Any failure to comply with these provisions may result in IT facilities being withdrawn.

ICT cannot be held responsible for the loss of elected members personal data and documents stored on Council devices.

What rules apply to my use of IT?

You must adhere to the Members ICT Usage Policy, which is detailed below:

The ICT usage policy applies to every individual who uses the Councils ICT facilities. It sets out what Council considers to be the acceptable use of those facilities. **It is essential that you have read and understood this policy completely. If you do not understand any part of this policy, please consult ICT for advice.**

Confidentiality (Applies to both Members and Officers)

- Maintain confidentiality. Do not leave your device anywhere where it is at risk of theft, or where unauthorised people may be able to read its contents. If you take equipment out of the home or office, keep it with you at all times, or lock it away securely and out of sight. Use a password lock for your tablet and mobile device, so that when they are idle for a defined period of time, they lock. Councillors leaving IT equipment in unattended vehicles, do so at their own risk and the costs of losing equipment this way could be recovered by deducting an amount from your Members Allowance or salary. Tablets will lock after 5 minutes if not used.
- Follow all instructions you are given to protect the confidentiality of information and do not leave information (on paper or on computer media) anywhere where it may be seen by someone not authorised to view it.
- Do not let anyone else use your personal login and do not reveal it to anyone.
- You must not access files, directorates or data, or log onto a computer using a user account which you have not been authorised to use.
- Do not copy or transmit data outside the Council except as authorised by the requirements of your role.
- Always remember that any emails or text messages sent to people outside of those on the Council’s network are not secure and may be viewed by others. Personal data should not be sent by unprotected email and if you are sending personal data, please use Egress or take advice from ICT on how it may be done securely.

Use of Email Services

The Council’s position on acceptable, unacceptable and forbidden use of email is defined at section 1.1 of the policy.

If you receive offensive or pornographic material from a known sender, where you yourself are offended by it or not, you should immediately and politely make the sender aware that you do not wish to receive any similar material and inform their manager (or ICT for Members). If the material comes from an unknown source, the message must be deleted immediately without a message being sent back to the originator.

Please manage your email box within the limits allocated to you. When you are notified that your mailbox is approaching capacity, kindly remove items to create more space. Please remember that you can save emails in personal folders if you prefer to keep them for reference but large attachments should be avoided.

Councillors are reminded that emails and data stored on the Council's network and servers, can be viewed if there is a requirement to do this and may be subject to disclosure under the Freedom of Information Act. This includes text messages sent using mobile devices. Please bear in mind when sending messages by these methods.

Internet use with Mobile Devices:

In accordance with the Councils acceptable use policy, it is acceptable to access reasonable non-business related web sites.

How can I get advice about any issues?

Please contact the ICT Helpdesk on 4142 / 01942 404142 or on Self-Serve

3.0 Monitoring

Wigan Council has a requirement to and reserves the right to monitor and keep records of any use of its ICT for a number of reasons relevant to the Council's business, including but not limited to:

- Ensuring compliance with this policy and other related Council Policies such as the Council's Code of Conducts for Employees and Members;
- Training and monitoring standards of service;
- Ascertaining whether internal or external communications are relevant to the Council's business;
- Preventing, investigating or detecting unauthorised or criminal activities through the use of the Council's ICT;
- Adherence to the General Data Protection Regulation and all other associated Data Protection legislation.
- Maintaining the effective operation of the Council's ICT system;
- Emails addressed to you which are received during your absence from work (e.g. due to sickness or holiday), may be reviewed by the Council, where there is a legitimate need to do so, authorised by the relevant Head of Service. This may inadvertently lead to the Council accessing personal communications to you.

Authorised officers may occasionally need to undertake activities that fall in to 'Unacceptable' or 'Forbidden' categories to carry out their daily work.

This is acceptable provided that it is done with the full knowledge and agreement of the internal audit services who have protocols to govern this. Such activities will be notified to the Assistant Director Strategic ICT Partnerships and will be undertaken in accordance with agreed protocols for this.

The Council fully appreciate that users have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy whilst in the work environment. However, all staff should take note that every person who uses the Council's ICT to send or receive information may have their communications intercepted and logged, even if it is marked as private or personal.

Wigan Council employs automated and manual monitoring techniques on many of their systems, including:

- Email recording, logging and filtering;
- Call, SMS and text logging (including content);
- Web content and URL logging and filtering;
- USB device monitoring;
- Anti-virus protection;
- Anti-hacking and anti-spy ware tools.

To ensure continued availability of the services and enable usage trend to be identified. It is clear from information that this delivers that the vast majority of users respect acceptable use.

ICT Security Team members legitimately accessing individual email will guarantee confidentiality except to the extent that is required to follow up breaches of policy, to comply with court orders or to facilitate criminal investigation.

Ultimately, Wigan Council is responsible for data held on equipment it provides and, therefore, must retain the right to monitor the content of such data for legal compliance.

4.0 Glossary of Terms

A number of terms are used throughout the Acceptable Use Code of Practice that may need explanation. These terms are defined below to further aid understanding.

ICT
ICT refers to system/applications, internet, email, mobile devices including telephones and mobile telephony devices, landlines, cameras and personal computers and servers.

Offensive
It is not possible to provide a definitive, prescriptive list of 'offensive' material. However the following identifies examples of the type of material that does fall within the definition of offensive throughout the acceptable use policy.

'Material that is defamatory, racist or discriminatory on grounds of religion, disability, gender or sexual orientation, or alternatively which is designed to harass, victimise or bully, cause pain or distress to individuals.'

Obscene
Literal definitions of 'obscene' describe material that is 'offensive/outrageous or repellent' or material that is 'designed to deprave or corrupt' the audience. For the purpose of this document, any material that will cause extreme offence to a Wigan Council employee, business partner or visitor will be considered obscene.

Compressed Files
Compressed files are ordinary files that have been changed so that they take up less space than the original file. These files when uncompressed can become extremely large and take up large amounts of space on the workstation or server. Commonly used compression tools are widely available and create files with a name extension of .zip.

Executable Code
An executable is a file that contains a program, i.e. a particular kind of file that is capable of being executed or run as a program in the computer. An executable file usually has a file name extension of .bat, .com, or .exe.

Limited Use
This is not prescribed and varies according to the amount of time which the employee has spent not undertaking their legitimate work.

An example would be a limited number of occasions, spread over a wide period of time – 1-3 occasions per week, for periods up to 10 minute each time, over a period of time.

Excessive Use
This is not prescribed and varies according to the amount of time which the employee has spent not undertaking their legitimate work. An example would be in excess of 3 times per week, for periods of more than 10 minutes each time, over a period of time.

Session
A session is the state in which a computer is left such that an interaction with connected resources can take place unhindered. Sessions are normally defined by a log on and log off action, or unlocking and locking a workstation using ctrl/alt/del keys.

Removable Media
Removable media consists of USB or Firewire memory sticks, mobile phones with the ability to connect as external drives, I-pods or MP3/4 players, floppy discs, CD/DVD/Blue-ray media, cameras, or portable or removable hard drives.

Adequate Protection or Encryption
Confidential, sensitive or personal information must be protected or encrypted using complex passwords of at least 8 characters of which at least 1 must be of numeric value.

For advice on how to do this please contact the ICT Help Desk on 4142 (01942 404142).