# Acceptable use of ICT Assets and Social media

April 2018

Appendix 1

Stronger Economy

Stronger Communities

Stronger Organisation

wolverhampton.gov.uk

CITY OF WOLVERHAMPTON COUNCIL

**INDEX**

## 1. Policy Statement

1.1 Any individual using ICT devices, assets and services to carry out Council business is deemed to have accepted this policy and is bound by it. Any breaches of this policy may lead to disciplinary action being taken.

1.2 The purpose of this policy is to ensure that:

- All users of the City of Wolverhampton Council's ICT assets are clear about what is acceptable and unacceptable usage of Council ICT assets.
- All employees are clear about what is acceptable and unacceptable usage of personal ICT devices during working hours.
- All employees are clear that ICT assets and the internet, with exception can be used for private use in non-working hours.
- All employees are clear about what is acceptable and unacceptable usage of social media.
- All employees are clear about how user activity is monitored to enable adherence to this policy.
- All employees are clear about the consequences of breaching this policy; and managers understand the process to manage breaches of this policy.

1.3 This policy does not include information on how to manage the risks associated with keeping data secure. Guidance on information security is provided in policies made available through the Information Governance framework, which can be accessed from the following link.

www.**wolverhampton**.gov.uk/igov

1.4 Reference is made to the risk of information leakage throughout this policy. Information leakage happens whenever a system or service that is designed to be closed to unauthorised parties reveals some information unintentionally to unauthorised parties nonetheless.

## 2. Scope

2.1 This policy applies to all City of Wolverhampton Council employees and persons representing the Council, including sub-contractors, consultants, Trade Union representatives, elected members and employees based in schools.

2.2 This policy applies to all aspects of ICT use, whether undertaken in a Council location or elsewhere, including the use of any separate standalone systems provided by the Council (or its ICT providers), or used to conduct business on behalf of the City of Wolverhampton Council. If, in any circumstances, privately owned ICT devices (commonly referred to as BYOD – Bring Your Own Device) and facilities are used when any of the above identified groups undertake business on behalf of the City of Wolverhampton Council, then their usage must conform to this policy.

## 3. Use of ICT assets

3.1 The term 'ICT assets' includes but is not limited to' all computing devices, such as (tablets, laptops, smartwatches, Ipads, PCs), telephones (land-lines and mobile phones), printing, scanning and photocopying devices (including multi-functional devices). It also refers to data storage, Information Systems, all software, networks, internet access and email systems.

### 3.2 Personal use of Council ICT assets

3.2.1 Access to social media and the use of work based facilities for personal business a privilege and not a right. This privilege is to be used responsibly. If not, used responsibly, the council, members of the public and employees will be put at risk.

3.2.2 Individuals may be held liable for the consequences of any misuse, even if this is accidental.

3.2.3 All ICT assets supplied by the City of Wolverhampton Council remain the property of the Council and are provided to conduct Council business.

3.2.4 You may make use of the Council's ICT assets for personal use and ~~of~~ the Internet in non-working hours.

3.2.5 When you are logged on to the Council's network there a few basic things that you are routinely prevented from doing:

- Accessing Council software and information that you are not authorised to use.
- Accessing certain kinds of internet sites and services such as:

  i) Those believed to contain inappropriate material. This includes Pornography, Gambling, Criminal Activity, Militancy and Extremist, Controlled Substances.
  ii) Those believed to pose a serious threat to the security of the Council's network, data and systems. This includes Webmail, Hacking, Phishing and Fraud.
  iii) Those believed to use technologies that can hamper the performance of the Council's network and systems and prevent colleagues from carrying out their duties effectively.

3.2.6 The Council uses commercial 'web site reputation' services to decide which Internet sites should be blocked. Examples at point 3.2.5 are not an exhaustive list and the nature of the Internet makes it impossible to cater for every eventuality. Therefore, contact the ICT Service Desk if:

- You are unable to access something that you think you should be able to access.
- You find that you are able to access an inappropriate site.
- You receive a security warning when trying to access a site. In this instance do not take further action until you have been advised by ICT.

3.2.7 You may use Council equipment for personal activities only if the device is attached to the corporate network. Personal content must not be stored on Council equipment or networks at any time. You should not use council supplied smartphones or laptop dongles to access the Internet unless it is for Council business. These devices connect through commercial mobile networks and the Council has to pay for the amount of data transmitted.

3.2.8 The Council will not be responsible for any losses incurred whilst using the Internet for personal use. This may be as a result of online banking, shopping or any other payment transactions.

3.2.9 Access to webmail services such as Google Mail, Hotmail and Yahoo is not allowed as viruses and malware are often transmitted as attachments to e-mail messages. In normal e-mail, these are picked up by the Council's anti virus systems before they reach your inbox. Webmail attachments cannot be scanned and they pose a very serious threat to the Council's systems.

3.2.10 You are allowed to use your Council e-mail address for very moderate personal activities and work related social communications. There is no guarantee however that these e-mails will remain private.

3.2.11 Do not use your council e-mail address if you register for Services or buy personal goods online. You may use your Council e-mail address to register for professional services such as news alerts relevant to Council business and professional forums and for membership of professional bodies.

3.2.12 Avoid using the same online accounts for both personal and professional activities. This can cause problems where a site – for example, Facebook requires you to register as an identifiable person, rather than sharing a business identity. Communications Team can offer advice on this if required.

3.2.13 Using computer facilities to download copyright material such as films, television programs and music tracks is not allowed unless the material is to be used as part of your work and you have the permission to do so. You must ensure that this material remains secure and is deleted from ICT systems once it is no longer required.

3.2.14 Communication facilities such as telephones, email, skype and social media accounts are provided for Council business. However, it is recognised that there are occasions when it is necessary to make or receive personal messages during the working day in an emergency situation, for example,

about a child care/ domestic emergency. Personal communications must be kept to a minimum.

3.2.15 Computer software is not permitted to be removed or copied from Council premises for personal use.

3.2.16 Photocopier, printers and scanners are provided for Council business only. They must not be used for personal use.

3.2.17 If work information is required to be saved to a memory stick then the stick should be obtained from ICT, who will advise on its's use.

## 3.3 Computing devices

3.3.1 When working in an agile manner, (in accordance with the SMART working protocol) ensure that you are aware of your surroundings and assess the risk of accessing the information you need to access (aligned to the Council's Information Governance policies); and, the security of your device.

3.3.2 Devices must not be left unattended and must not be vandalised (including writing on or defacing equipment).

3.3.3 All reasonable steps must be taken to secure devices. If not, then individuals may be held responsible for replacement costs where neglect can be shown causing damage, loss or theft.

3.3.4 The loss or theft of a device (to include personal devices used for Council business) must be reported to the police as soon as possible (within 24hrs). Obtain a crime number or lost property number and note the Police Station reported to, telephone number and the station officer's name. Inform ICT immediately ICT.Servicedesk@wolverhampton.gov.uk or by calling 01902 (55) 8000 as soon as possible.

3.3.5 The procurement and installation of hardware over and above the hardware assigned to you by your manager in conjunction with ICT is not permitted without prior consultation with business managers and ICT.

3.3.6 ICT keep software equipment up to date by regularly using patch devices to ensure that security standards are maintained.

## 3.4 Mobile devices

3.4.1 In line with legislation, drivers of any vehicle must not use a hand-held mobile phone or similar handheld device whilst in control of the vehicle. This includes periods when the vehicle is stationary. In line with legislation, "hands free" usage is permitted, but only if the driver is not distracted and in control of the vehicle.

3.4.2 The use of mobile devices must not introduce risk to yourselves or others. Ensure that you are aware of your surroundings and assess the risk of

using a mobile, including the risk of using head-phones. Please also refer to the health and safety mobile phone policy; which can be accessed from link below.

http://portal/corporate/healthandsafety/Documents/Mobile%20Phone%20Safety%20Arrangements.doc

3.4.3 Data held on mobile devices, including multi-media, must comply with Information Governance and business specific policies.

3.4.4 In the event of a Council provided mobile being lost or stolen beyond the hours of 08:00 – 18:00 Monday – Friday, please advise Vodafone direct on 07836 191 191. If you have had to call Vodafone direct, please ensure you contact ICT to advise them of your actions or ICT in normal office hours as soon as practicable.

3.4.5 Premium rate calls are not permitted from Council owned mobile telephony devices.

3.4.6 Mobile device and sim cards must only be used in conjunction with the device or sim they were purchased for use with. Removal or exchanging devices and sims will affect the warranty which may result in limited or no support from our 3rd party supplier for faults or for barring/suspending of devices following loss or theft.

3.5 **Personal mobile devices**

3.5.1 The term 'personal ICT devices' includes, but is not limited to' all computing devices that are not managed by the City of Wolverhampton Council ICT service, to include tablets, laptops, mobile phones and memory sticks/cards.

3.5.2 With discretion of the manager, reasonable use of a personal mobile phone is permitted for making or receiving calls/messages in the event of an emergency or for exceptional reasons. Phones must be set to 'silent mode' during work hours and any usage must not disturb colleagues. If a local arrangement is in place which requires that mobile phones cannot be on show, then that agreement needs to be complied with.

3.5.3 In cases where a manager considers that an employee is making or receiving an unreasonable amount of personal calls or text messages during working hours, they are permitted to reasonably request that the employee turns off their phone/ device during working hours. This includes using the phone/device for any non-work reason.

3.5.4 No Council data (to include multi-media) must be created, stored or saved on personal devices including memory expansion cards (e.g. SD cards, MicroSD cards, etc.) in line with Information Governance policies.

3.5.5 No attempt must be made to connect your personal device (for example by cable, Bluetooth, USB or wireless) to any networked laptop or desktop PC

for data sharing purposes, as this creates a risk to the security of the Council network; and also creates an information leakage risk.

3.5.6 Personal mobile devices can be used as a mobile 'hot spot', by tethering to Council devices to enable access to Council services when working in an agile fashion. However, if any costs are incurred by your mobile provider, these must be paid by the employee, not the Council.

3.5.7 Council content made available on personal mobile devices, must only be accessed through secure channels provided by ICT. In instances such as these, ICT will need to install a secure mobile device management solution on personal devices. In the event of loss or theft, Council content will be remotely wiped. Whilst ICT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

## 3.6 Systems, software and applications

3.6.1 Systems, software and application licensing agreements must be abided by. These are held by ICT Services and Business owners. When software is purchased by the Business, they provide a copy of the license to ICT to add to the inventory. Licensing referring to devices and applications i.e. Office 365 are managed by ICT. If an account or device is deleted the license is removed.

3.6.2 In line with national security standards, all systems, software and applications accessed from Council devices needs to be licensed and supported so that they are kept up to date with any security updates. It also needs to adhere to secure data storage standards. This means that any system, software or application needs to be assessed before it can be added to the network, device or the 'app store' by ICT.

3.6.3 Loading or copying licensed software across the network to other computers requires prior approval from business managers and ICT.

3.6.4 Hacking is the unauthorised access to or control over computer network security systems for some illicit purpose. "Hacking" into any program or data files, breaking license numbered applications or attempting to subvert or circumvent system, application and network security measures is not permitted.

3.6.5 The procurement and installation of additional systems, software and applications over and above those programs assigned to you by your manager in conjunction with ICT is not permitted without prior consultation with business managers and ICT.

3.6.6 To prevent information leakage, Council content made available through web-browsers or Council applications must not be saved on personal devices, or shared through personal applications, in line with Information Governance policies.

3.6.7 To prevent information leakage on a shared device, for example a family computer, you must only access Council content made available through web-browsers or Council applications using an account that is not accessible by any other person. This is because logon credentials can be saved locally resulting in an automatic login to Council information.

3.6.8 Skype

- To prevent information leakage, document attachments and screenshots with Council content on them must not be shared in Skype discussions or meetings, in line with Information Governance policies.

3.6.9 Microsoft Office 365

- Office 365 functionality can be accessed through a web-browser from personal devices, to include emails and documents.

- To prevent information leakage, Council Office 365 content must not be saved on personal devices, or shared through personal applications, in line with Information Governance policies.

- To prevent information leakage on a shared device, for example a family computer, you must only access Council Office 365 content using an account that is not accessible by any other person. This is because logon credentials can be saved locally resulting in an automatic login to Council information.

3.6.10 Mobile applications

- Where mobile applications used for Council business are made available for use on personal devices, Council content made available through these applications must not be saved on personal devices, or shared through personal applications in line with Information Governance policies.

- To prevent information leakage on a shared device, for example a family computer, you must only access Council application content using an account that is not accessible by any other person. This is because logon credentials can be saved locally resulting in an automatic login to Council information.

3.7 **Network usage, to include WiFi, data cables and mobile 'hot spots'**.

3.7.1 Council provided networks:

- ICT provides WiFi and fixed (services accessed over a data cable) networks to different user groups, to include Council employees (corporate network) and members of the public (public network) to access Council services.

- Only authorised devices can be connected to the corporate network,

aligned with Information Governance policies.

- Public network services are provided for members of the public, partner and third parties to access the internet and any other services provided over this network, for example printers.

3.7.2 Third party networks

- Council ICT services can only be accessed over public and private networks when using the secure, remote access services provide by ICT, aligned with Information Governance policies.

- If accessing Council services from shared, public devices, ensure that any cache/ history is cleared to prevent information leakage. (clear search history)

- When working in an agile manner, using third party networks, ensure that you are aware of your surroundings when accessing the information you need to access (aligned to Information Governance policies); and also the security of your device.

3.7.3 **Tethering to mobile 'hot spots'**

- Personal or Council provisioned mobile devices can be used as a mobile 'hot spot', tethering to Council devices to enable access to Council services when working in an agile manner.

- If using your mobile phone as a mobile 'hot spot' (either personal or provided by the Council), ensure that you are aware of your surroundings when accessing the information you need to access (aligned to Information Governance policies); and also the security of your device.

- Tethering increases the regularity with which you need to recharge your battery and also increases data usage (and associated cost) so must not be used to meet every day working requirements.

3.8 **Internet usage**

3.8.1 Using Wifi at Home

ICT do not provide WiFi connectivity to home location. If you wish to use your device at home then you will need to use this with your own WiFi connectivity. Alternatively, you can use your personal mobile or council provided mobile as a mobile hotspot but this has an impact on data usage. This has a cost associated and so should not be used as a method of connectivity to meet every day working requirements.

ICT aims to ensure appropriate access to and use of the Council's internet facility to mitigate the following risks:

- Viruses and other malicious software. (malware)
- Service disruption.
- Potential legal action and/ or fines against the Council or individual(s).
- Damage to the Council's reputation.
- Inappropriate use of Council resources.

3.8.2 The Council uses commercial "web site reputation" services to decide which Internet sites must be blocked. Reputation services monitor web sites and categorize them according to their content (e.g. "government", "sport", "shopping", etc.). ICT blocks access to specific categories. The Web is such a big and dynamic place that sites can be put into the wrong category by the reputation service. Individual sites may be unblocked by request regardless of their category. The nature of the Internet makes it impossible for such services to be perfect. Therefore, contact the ICT Service Desk (http://portal/corporate/ict/selfhelp/Pages/home.aspx) if:

- You are unable to access something that you think you must be able to access.
- You find that you are able to access an inappropriate site.
- You receive security warnings when trying to access a site.

Access to sites that are blocked will be referred to Business Managers for approval.

**3.8.3 Guidelines**

- Do not use the browser's facilities to store personal logon ids and passwords, or to pre-fill online forms.

- Do not tick options to "keep me logged in" at web sites where you have personal accounts. These options are often ticked by default when you go to the web sites, so you may need to un-tick them.

**3.9 Unacceptable use of ICT assets and resources**

3.9.1 Using the internet, email or other communication channels to send messages which give the impression that you are representing, giving opinions or otherwise making statements on behalf of the Council unless expressly authorised to do so.

3.9.2 Using the internet, email or other communication channels to send defamatory, threatening, racially and/ or sexually harassing or obscene messages to other employees or external parties.

3.9.3 Using ICT assets and resources to download or distribute illegal software, pornographic, violent, racial or harassing material.

3.9.4 Using ICT assets and resources for unlawful or immoral purposes, or to assist with such purposes.

3.9.5 Overloading computer facilities with excessive data or known time-intensive procedures. You and your managers will be contacted by ICT if you have excessive data in your personal messaging or file stores. In emergencies, if the volume of your data or the actions you are performing compromises Council services, ICT may delete data or intervene without your consent.

3.9.6 Carrying out activities that unreasonably waste ICT resources (to include employee resources) or activities that unreasonably serve to deny ICT services to authorised users. i.e. putting in place unnecessary obstacles to hinder delivery of any ICT Services.

3.9.7 Carrying out activities that conflict with a user's obligations to the Council, to include the delivery of Council services and adherence to core values.

3.9.8 Attempting to connect unauthorised devices to Council networks.

3.9.9 Carrying out activities using ICT assets and Social Media that are in breach of Information Governance policies.

## 4. Use of Social Media

4.1.1 Any use of Social media applications for progressing work related tasks has to be in line with Information Governance policies. The respective Head of Service and Corporate Communications Team need to be made aware of its use.

4.1.2 Social media applications include, but are not limited to:

- Social networking sites e.g. Facebook, Instagram, LinkedIn.
- Video and photo sharing websites e.g. Flickr, YouTube.
- Micro-blogging sites e.g. Twitter.
- Weblogs, including corporate blogs, personal blogs or blogs hosted by on-line media publications.
- Forums and discussion boards such as Yammer, Yahoo! Groups or Google Groups.
- Online Encyclopaedias such as Wikipedia.

Any other websites that allow individual users or companies to use simple publishing tools. Social media applications are not limited to websites and this policy applies to any other electronic application (such as mobile phone based, or hand held device based applications) which provides for the sharing of information to user groups or the public at large. Online communications may include posting or publishing information via Social Media Applications, uploading and/ or sharing photos or images, direct messaging, status "updates" or any other form of interaction and/ or communication facilitated by social media.

4.2 **Personal social media accounts – guidelines**

4.2.1 Revealing or implying a place of employment potentially increases exposure to both the individual and the Council. Individuals are responsible and accountable for information that they post and put forward and must monitor their posts accordingly. Employees, particularly those who work closely with Service users are expected to maintain a professional image at all times.

4.2.2 Disparaging or adverse comments about the Council, employees, contractors or colleagues must not be made. Under no circumstances should employees share confidential information arising from their employment with the council.

4.2.3 Material posted by others with inappropriate or disparaging content and information stored or posted by others (including non-employees) in the social media environment may also damage the Council's reputation. If you become aware of any such material which may damage the Council or its reputation, you must immediately notify the Council's Communications team.

Work email addresses must not be used to set up personal social media accounts. Do not use your Council email address if you register for services or buy personal goods online. You may use your Council email address to register for professional services, such as appropriate news alerts and professional forums and membership of professional bodies.

4.2.4 Avoid using the same online accounts for both personal and professional activities. Employees and volunteers must ensure that social media interactions are professional, appropriate and in line with Council safeguarding policies (e.g. is it appropriate to accept or send friend requests.

4.2.5 Access to webmail services such as Google Mail, Hotmail and Yahoo is not permitted from Council devices. This is due to the risk of information leakage from the Council network, aligned to Information Governance policies.

4.2.6 **External File Sharing** –

Employees should not upload Council documents to external file-sharing or collaboration services unless:

- Employees understand the terms and conditions of using the service, including how your information is used by the service provider and the legal liabilities for disclosure of information in compliance with the General Data Protection Regulations.
- Employees are completely confident that the material you are uploading is appropriate for release to the public domain, even if releasing it is not your intention.

- Employees know which country the information would be stored in, and the location is compliant with relevant UK and EU legislation
- Employees know that you can permanently delete the material from the service.

4.2.7 Yammer, LinkedIn and similar services are aimed at professionals. Employees must treat these services with as much caution as other "free" services. In particular, be aware that such services often try to copy your contacts list from Outlook or your phone, in which case information may be disclosed about other people.

**4.3 City of Wolverhampton Council social media accounts – Principles of use**

4.3.1 All use of Council social media accounts must be in accordance with the council's objectives and values, its Code of Conduct for Employees, the Email, Information Governance, Equal Opportunities and Dignity at Work policies and procedures.

4.3.2 Employees must not set up any council social media accounts without the prior engagement and agreement of the Corporate Communications Team and approval from their appropriate Head of Service.

4.3.3 Employees with responsibility for council social media accounts, known as account moderators, must inform the Corporate Communications Team of any changes to account passwords or account moderation.

4.3.4 Account moderators must only engage with appropriate accounts linked to the council's day to day business and not personal interest such as football clubs and celebrity accounts.

4.3.5 All council accounts must have clear council branding, approved by the Corporate Communications Team.

4.3.6 Account moderators who publish on council social media accounts are indemnified for posts published as long as they have received instructions or information and acted in good faith. The moderator needs to ensure the accuracy of the information or to ensure that the person asking for the information to be published is authorized to do so.

4.3.7 Account moderators must act in accordance with the council's Data Protection and Information Security policies.

4.3.8 Account moderators must act professionally at all times in council social media accounts. All posts must be in line with the council's values and the Employee Code of Conduct.

4.3.9 Content copied from elsewhere, for which the council does not own the copyright, must not be published.

4.3.10 Account moderators must not publish the same or similar content repeatedly or in bulk, this can also be called "spamming".

4.3.11 Council social media accounts must not be used at any time for political purposes or political party campaigning.

4.3.12 Account moderators must regularly review the council accounts they are responsible for. Any inappropriate content must be removed immediately and the Account Moderator must report the content to their line manager, Corporate Communications and directly with the social media site or application.

4.3.13 Accounts moderators must not post promotional content for commercial organisations or endorse external organisations, unless it has been approved by the appropriate Head of Service and Corporate Communications have been consulted.

4.3.14 Account moderators must not use the same passwords for social media accounts that are used to access council computers or devices.

4.3.15 Account moderators must not follow links or download software on social media pages posted by individuals or organizations that you do not know.

4.3.16 If any content on any social media web page looks suspicious in any way, account moderators must close their browser and must not return to that page.

4.3.17 Accounts, moderators must configure social media accounts to encrypt sessions whenever possible. Facebook, Twitter and other support encryption as an option. This is extremely important for roaming users who connect via public Wi-Fi networks.

4.3.18 If a device that is used to access council social media accounts is lost or stolen, Corporate Communications must be notified immediately so that passwords can be changed.

4.3.19 Roles and responsibilities

- Line managers are responsible for ensuring that account moderators and any social media accounts within their control are monitored effectively and operate within this policy and code of practice. All managers are responsible for ensuring that those in their teams understand this policy and abide by it, and for giving guidance on the appropriate use of social media sites in the workplace. Line managers must also inform Corporate Communications about any changes to the management of accounts including change of account moderators and passwords.

- Account moderators are responsible for the effective operation of council social media accounts in line with the policy and code of practice, following approval and support from Corporate Communications. On receiving access to social media all account moderators will be asked to sign a declaration and affirm their acceptance of the Social Media Policy and principles set out in the

Social Media Code of Practice and will be regularly reminded of the consequences of failing to uphold them. Failure to acknowledge acceptance of these principles will result in access to social media facilities being denied.

- Corporate Communications are responsible for approving Council social media accounts and will maintain a record of all accounts, their moderators and passwords.
  They will also support the initial development of council accounts and monitor accounts using a social media monitoring application and will be responsible for advising on the appropriate use of the social media.

## 5. Policy monitoring and privacy

5.1 From September 2017 ICT have made changes to strengthen the authority's network passwords.

The following rules are now in place:

- Passwords must not contain words or common phrases from the Oxford Dictionary.
- Passwords must not contain the current year date – 2017.
- Passwords must not contain part of words, for example: Laptop. This would not be acceptable and would have to be changed to L@pt0p or similar, as lap and top are both words.

5.2 Below are best practices ICT strongly encourage all employees to follow:

- Do not share your password with any other person.
- Never use the same password for work accounts that you use for personal accounts.
- Never use the 'remember password' option on shared computers, laptops and tablets.
- Do not store passwords electronically unless there is encryption.
- Your password should not contain personal information such as name, company name, street name, date of birth etc.

5.3 Investigating or detecting unauthorised use of the Council's ICT: all email, Skype, internet use, telephone calls and other ICT usage is logged and may be subject to automated monitoring. Monitoring may be carried out in compliance with applicable obligations under the Data Protection Act 1998 (and in compliance with the General Data Protection Regulations (EU) 2016/679) and where this is permitted under the Regulation of

Investigatory Powers Act 2000 (and associated regulations) for the purposes of:

- Preventing or detecting criminal activities.
- Investigating or detecting unauthorised use of the Council's ICT facilities.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures and standards.
- Ensuring effective system operation.

5.4 Individual emails, skype conversations or file stores may need to be accessed by an ICT or business manager, following authorisation by a senior manager, to ensure Council services can continue in the event of absence or investigation.

5.5 ICT has the right to audit, retract, monitor or report on the usage of ICT resources to assure compliance with this policy within the parameters of current Privacy laws.

5.6 Any ICT activity may be recorded passively. This is data that ICT systems routinely accumulate as a by-product of any action or event, in logs, caches, web histories, browser cookies, most-recently-used lists, search indexes, audit records, and so on. The corporate ICT infrastructure also logs things that are happening to maintain performance and diagnose problems.

5.7 When you leave the employment of the Council, all data stored in your Council ICT account (including emails and documents) may be made available to your line manager and possibly to other Council employees in line with Information Governance policies.

## 6. Policy exceptions

6.1.1 Where, for operational reasons, an exception to this policy is required a request must be submitted through the ICT Service Desk. (http://portal/corporate/ict/selfhelp/Pages/home.aspx). The request and associated risk will be reviewed by both business and ICT managers before approval.

## 7 Managing policy breaches

7.1.1 Any breaches of this policy may result in disciplinary action being initiated.

7.1.2 Where there is evidence of a criminal offence, the issue will be reported to the Police (or relevant statutory body) for their action. The Council will co-operate with and disclose copies of any data stored, appropriate logs and any hardware used (relevant to the investigation) to the Police (or relevant statutory body) and other appropriate external agencies in the investigation of alleged offences, in line with current legislation.

## 8. Links to other Policies and Procedures

8.1 This policy must be read in conjunction with: Information Governance policies:www.**wolverhampton**.gov.uk/igov

Health and Safety mobile phone policy:

http://portal/corporate/healthandsafety/Documents/Mobile%20Phone%20Safety%20Arrangements.doc

## 9. Responsibilities

9.1 Employees

9.1.1 Employees are expected to read and understand this policy and to speak to their manager before using any computer equipment or services if there is anything that they are not sure about.

9.2 Managers

9.2.1 Managers have a responsibility to ensure that their employees are aware of this Policy, understand it, accept its provisions and abide by it, and that sanctions can be imposed for breaches of policy. This may lead to disciplinary action being taken against the employee.

9.2.2 Managers must advise employees on acceptable use if they have queries.

9.2.3 Managers should ensure that all IT equipment issued to employees is listed as an asset on agresso – personal details. ICT also keep a master list of all ICT assets distributed to employees.