West Berkshire Council ICT Policy
and
ICT User Usage Agreement

Document Control

Document Ref:		**Date Created:**	13th December 2010
Version:	2.0	**Date Modified:**	29th April 2011
Revision due	April 2013		
Author:	Kevin Griffin		
Owning Service	Information & Communications Technology (ICT)		

Change History

Version	Date	Description	Change ID
0.1	01/12/2008	Document Created	
0.2	02/03/2009	Revised document following peer review	
1.0	14/04/2009	Policy agreed for publication by Corporate Board	
2.0	29/04/2011	Review to cater for various amendment requests (Approved by ICT Strategy Board January 2011)	

This Policy is not for publication externally

Contents

1. Purpose of the ICT Policy

1.1 The purpose of this policy is to ensure the effective and appropriate use of Information and Communications Technology (ICT) by and within West Berkshire Council.

1.2 The aim of this policy is not to impose unreasonable or unnecessary restrictions but rather to ensure that everyone using West Berkshire Council's ICT are fully aware of the rules surrounding its use.

1.3 This document is published separately as well as being incorporated into the WBC Employee Handbooks.

1.4 This Policy has had consultation with Heads of Service and Trade Unions and has been ratified by the Council's Corporate Board and Management Board.

2. Applicability

2.1 This Policy applies to:

2.1.1 All people (hereafter referred to as Users) using West Berkshire Council owned, or leased, ICT equipment, systems, or data whether this be from work, from home or from other non-Council location. This will include non-schools Council employees, Elected Members, Consultants, Agency staff and Contractors working for the Council and external organisations working with the Council, whilst engaged on Council business.

2.1.2 This policy does not apply directly to users in West Berkshire Schools, except where schools staff are accessing WBC systems e.g. Agresso or the WBC Intranet. Each School is expected to implement and maintain its own Acceptable Use Policy for ICT.

2.2 ICT equipment, systems and data referred to in this policy include: -

- Personal Computers (PCs) including desktops, laptops and tablets and associated peripherals such printers, external drives etc.
- Telephones and telephony equipment including fixed-line telephones, mobile phones, VoIP 'soft' phones, 3G data cards and fax machines
- Handheld devices such as BlackBerries, PDAs etc.
- Any software application or database run by, or for, West Berkshire Council
- Any system or server run by, or for, West Berkshire Council
- Other computer hardware including memory sticks, digital cameras

3. Responsibilities

3.1 It is the responsibility of all users identified in Section 2.1.1 above to familiarise themselves with and to comply with this Policy and the incorporated ICT *User Usage Agreement.*

3.2 Compliance with this Policy is a condition of working for the Council or using its ICT equipment or systems.

3.3 All managers are directly responsible for implementing this Policy and any related procedures within their service areas, and for the adherence of all users within their area.

4. Policy

4.1 It is the policy of West Berkshire Council to ensure that its ICT equipment, systems and data are used effectively and efficiently for the needs of the Council and are not misused.

4.2 The Council has a duty to protect the availability, integrity and security of ICT equipment, systems and data within its charge.

4.3 This policy will be also be supported by the development and publication of additional standards, procedures and guidance documents where appropriate.

5. Appropriate Use of ICT

5.1 All users of WBC ICT shall:-

- comply with all laws pertaining to the use of ICT. Current relevant acts are listed at Appendix A to this document.
- comply with all relevant WBC standards linked to the use of its ICT systems and data.
- Comply with the Council's Financial Regulations regarding procurement and control of ICT assets.
- use ICT only for lawful activities (in accordance with United Kingdom and International law).
- take reasonable measures to safeguard the physical security of business equipment they use.
- take reasonable measures to prevent unauthorised access to systems and information that they use. These measures will include, but are not limited to:-
  - safeguarding passwords and changing them regularly
  - not letting others use equipment, or access systems or accounts assigned to them
  - not removing security measures, or allowing others to do so
  - logging out of, or locking systems when they are left unattended
  - avoiding copying any sensitive data extracted from ICT systems to other media e.g. removable disks, memory sticks, shared drives
  - safeguarding printed information extracted from systems
  - not sending sensitive data outside of the organisation except when using approved secure means
- abide by the rules of the ICT User Usage Agreement.

6. Misuse of ICT

6.1 Users of WBC ICT facilities shall not:-

- use ICT to engage in any criminal activity
- use ICT to access or distribute any unsuitable materials (e.g. racist, pornographic, media promoting violence etc.)
- wilfully try to access systems or information for which they are not authorised, or to assist others to do so
- fraudulently use or access any system or information, or fraudulently amend any records
- use the Council ICT systems for their own business purposes, or for monetary gain
- knowingly infringe copyright laws
- switch off, bypass or ignore security controls or restrictions
- take actions that waste time or resources (e.g. sending unsolicited emails to large groups of people)
- make inappropriate or excessive use of Council systems for private or non-council use.

7. Privacy

7.1 The Council provides ICT facilities for the effective sharing of information between employees and its external suppliers, partners and customers. These facilities are provided to support the Council's business and as such any information created or input to the Council's systems (e.g. email messages) are and remain the property of the Council.

7.2 Such information is not the private property of any individual nor shall any individual expect there to be any personal privacy with respect to any such information, whether it be designated "private" or not.

7.3 Whilst not routinely monitoring an individual's use of ICT the Council maintains the right to review, audit, intercept, access, monitor, delete or disclose any information, created, sent, received or stored on its ICT systems for any purpose.

7.4 Use of the Council's systems by any person identified in Section 2.1.1 implies that the user recognises and consents to the rights of the Council described above. Therefore, users should have no expectation that any electronic information on WBC's ICT systems will remain private.

7.5 In so far as is allowed by the Human Rights Act, managers may request access to information produced (e.g. emails) by staff or agents within their service, or request usage statistics on individuals (e.g. for time spent on the internet, sites visited, phone calls made etc.). Such a request would be authorised by HR and would normally be conducted by the ICT Service.

8. Failure to comply with the WBC ICT Policy

8.1 This document together with the *ICT User Usage Agreement* and other relevant published standards and procedures provides ICT users with essential information regarding the acceptable use of ICT in WBC and sets out conditions to be followed. It is the responsibility of all to whom this policy applies to adhere to these conditions. Failure to do so may result in;

- withdrawal of access to relevant services
- informal disciplinary processes
- formal disciplinary action (in accordance with the Council's disciplinary procedure.

Additionally if a criminal offence is suspected the Council may contact the police or other appropriate enforcement authority to investigate.

9. Review

9.1 This policy will be reviewed to respond to changes and at least every two years.

9.2 The ICT Strategy Board is responsible for reviewing and maintaining this Policy.

9.3 Corporate Board and Management Board are responsible for approving updated policies.

All prior sections comprise the WBC ICT Policy

All following sections comprise the WBC ICT User Usage Agreement

10. Good Practice

10.1 All users of WBC ICT shall:-

- Safeguard access by protecting passwords
  - — create and use password that are not easy to guess or crack
  - — use passwords with a minimum length of 8 characters containing both upper and lower case letters and at least one numerical digit
  - — not use names, or dictionary words
  - — avoid details personal to you that might be known e.g. spouse's name, birthday, favourite football team etc.
  - — keep passwords confidential
  - — avoid keeping a paper record of passwords
  - — change passwords regularly (at least every 90-days), and whenever there is any indication of possible compromise

- only store information and files in approved 'safe' locations i.e. the relevant corporate business systems such as Raise, Uniform etc. Where available within an EDRM system, or on WBC network locations such as H: drives, I:drive or G: drive which are all subject to routine daily backups.

- avoid storing files on 'local' drives i.e. the hard drive C: drive of a desktop or laptop PC. Where files are stored locally staff must take responsibility for the security of the information and for creating backups.

- never copy sensitive information on unencrypted 'local' storage such as unencrypted memory sticks, or CDs due to the risk of the data being lost or stolen.

- perform regular housekeeping on their computer records and information (e.g. by deleting files and emails etc. no longer required).

- ensure that they have received the appropriate training to use their equipment and software safely and effectively.

- report faults, especially those that might compromise data security or integrity, to the ICT Help Desk in a timely manner.

- report actual or suspected security leaks or breaches, equipment or information loss to their line manager and the ICT Help Desk as soon as they have occurred.

11. Use of the Internet

11.1 West Berkshire Council accepts that the Internet is very useful for quickly and easily accessing and researching information and keeping up-to-date with news and professional development, etc. Government departments and professional bodies have websites which contain information which is vital to many of us to carry out our jobs effectively, and some Council officers need to monitor the content of sites. It is therefore an essential tool provided to most of WBC's ICT users.

11.2 The Council also recognises that users may, from time to time, need to access the Internet for personal reasons during the span of the working day. Users are therefore allowed to access non-work sites within reasonable limits in accordance with the following code of practice:-

- **DO NOT** use the Internet, in normal circumstances, to access websites other than for work purposes during core working hours, except with the express permission of your line manager. There may be some websites (e.g. travel news) which you may legitimately need to access during core working hours to get important information which will affect your work-life balance. If you need to do this, you should restrict the time spent on the website to no more than a few minutes. If you are in any doubt about accessing non-work related websites during the working day, you should discuss this with your manager.

- **DO NOT** use the Internet to access or update your own personal social networking websites (e.g. Facebook) or to access any other recreational sites during core working hours, as doing so means that you are wasting time for which you are being paid by the Council. Access to corporately provided Facebook pages e.g. Youth Services are exempt from this restriction.

- **DO NOT** spend excessive time accessing personal email such as Hotmail. Very limited personal use is acceptable (i.e. no more than a few minutes a day), but line managers have the discretion to withdraw this permission if it is abused.

- **DO** use the Internet to access non-work related sites for personal reasons during your lunch break or before or after you have completed your working hours for the day. However, check before doing so that this is operationally convenient in your work area. You should always 'clock out' of your flexitime recording system (or the system that is in use in your work area) before using the Internet for non-work purposes.

11.3 It is important that access to the Internet in WBC is used responsibly and legally. Users must not take any action which could bring the Council into disrepute, cause offence, interfere with individual's or the organisation's work or jeopardise the security of the Council's ICT systems, software or data.

11.4 The Council controls Internet access by monitoring and filtering to protect both individuals and the organisation. Users must only access the Internet through the links provided. Any attempt to access through dial-up accounts, or to switch-off or otherwise bypass the controls in place is prohibited.

- **Internet Monitoring** - The Council's proxy server system automatically monitors the amount of time spent on the Internet and the sites accessed. This enables the Council to produce reports on Council-wide internet use and the type of sites being accessed, as well as detailed reports on Internet usage by individual employees. Such information will not be routinely disclosed to managers, but may be requested in specific circumstances as part of an investigation into potential misconduct, including breach of the ICT Policy. If a report is to be requested from ICT the line manager will normally inform the employee as part of the investigation process.

- **Internet Filtering** – The Council's proxy server system is configured to block access to sites containing offensive, illicit or potentially dangerous information including, pornographic material, racial hatred or religious hatred, or other discrimination or hatred, sites involving or promoting violence or illegal acts. The filtering system also protects WBC against potentially harmful files such as computer viruses by preventing the download of certain types of files. Other sites such as gambling, file sharing sites etc. are also blocked. **DO NOT** attempt at any time to access websites in any of the blocked categories defined above.

11.5 Users must be aware that no protection system is 100% guaranteed and that they may still inadvertently gain access to unacceptable, offensive or other normally blocked materials. People inadvertently accessing offensive material when accessing the Internet should inform their manager and the ICT Help Desk immediately. Accidental access will not normally result in any disciplinary action but failure to report it may do so.

11.6 Staff who have to monitor offensive material as part of their jobs, e.g. Child Protection, Equal Opportunities and Trading Standards, may be granted access to relevant material with the permission of their Head of Service. Permission must only be given to named individuals and a record placed in their personal files.

11.7 Users shall not attempt to download or install unauthorised software from the internet.

11.8 Users should be aware that, as with other information sources, not all information on the Internet is accurate, complete or reliable. Users should independently ensure its validity, and their rights to use it , before making use of it for Council business.

11.9 Staff shall not bypass the Council's internal procurement procedures by buying items for the Council over the Internet. There may be occasions where purchasing items over the internet is the only, or best option. In these cases users should obtain the authority of the manager, Head of service and procurement Service where appropriate.

12. Use of Email

12.1 Email is now a primary form of communication both within the Council and externally to its partners and customers.

12.2 WBC's standard corporate email system now provides the facility to send secure encrypted email by preceding the Subject title with [Secure]. This functionality should always be used when sending sensitive or confidential information by email, particularly where it is been sent to an external email address.

12.3 An email message will have the same legal status as any other written document and must therefore be treated in the same way as any other formal business correspondence.

12.4 WBC email users should conform to the following code of practice:-

- **DO** use meaningful subject title to help the recipient gauge the relevance and importance of each email they receive

- **DO** check spelling and grammar as you would other written communications

- **DO** check emails regularly and delete old or unwanted emails in your mailbox

- **DO** implement an out-of-office rule or provide delegated access to your email when you will be away from the office to ensure no important messages are ignored or delayed

- **DO NOT** send any emails which are unlawful or which breach any Council standards or policies or are not aligned with the Council's values. This includes messages that may harass or offend someone. Harassment can take the form of argumentative or insulting messages or any other message that the sender knows or, or might reasonably be expected to know, would cause distress to a recipient.

- **DO NOT** breach privacy by forwarding information known to be confidential or sensitive, or likely to upset or offend the recipient without the consent of the original sender.

- **DO NOT** send emails from someone else's account, except under proper delegated arrangements where individual accountability is retained, as this may constitute impersonation or misrepresentation of another individual.

- **DO NOT** send emails from non corporate accounts e.g. hotmail, yahoo etc. containing official WBC business. These accounts are outside of the control of the Council and are not secure.

- **DO NOT** copy people in to emails unless considered essential and do not reply to all when a reply to sender will suffice.

- **DO NOT** send emails to distribution groups e.g. All Market Street Users inappropriately. There are others means of disseminating messages about charity events, staff leaving etc. that do not waste other user's time checking unsolicited email. Certain Groups such as All Users are restricted so that only certain nominated staff are able to use them.

13. Use of Telephones/Telecommunications Equipment

13.1 This section covers the use of WBC telephones/telephony equipment that fall into 3 main categories, namely fixed (desk) phones, mobile phones (including BlackBerries) and ‘soft’ IP phones. Some policies are applicable to all phone types whereas others are applicable only to a particular phone type e.g. mobile phones.

13.2 General

13.2.1 Users shall not try to bypass any security measures or cost controls in place on their telephony equipment without prior consent from their line manager and the WBC Telecoms Team.

13.2.2 WBC telephony equipment is provided to help users engaged on Council business conduct their daily work. Personal use of this equipment should be avoided and where personal usage is deemed excessive by the Council users may be asked to reimburse costs incurred by the Council.

13.2.3 Users shall accept that their WBC telephone contact details will be included and published by corporate systems such as Outlook and the Intranet for the ease of other users.

13.2.4 Users shall answer their telephone in accordance with the relevant performance standard for the Council or within their service.

13.2.5 Where voicemail is used it must not be viewed as an alternative to answering the telephone and voice mailboxes must be checked on a regular basis.

13.2.6 Managers are responsible for ensuring their staff meet the required telephone answering standards and for monitoring telephone usage and call costs for their service areas. The WBC Telecoms Team provide monitoring facilities and regular reports to help managers to fulfil this responsibility.

13.3 Desk Phones

13.3.1 Desk phones should not be plugged or unplugged from the corporate network without the prior knowledge and approval of the WBC Telecoms Team.

13.3.2 Desk phone telephone usage is controlled i.e. users cannot dial premium rate or international number, and monitored to measure performance and to track call destinations, duration and costs.

13.3.3 Desk phones are not secure and could be used by anyone. WBC staff shall not use another persons phone to knowingly defraud or bypass controls. Staff should report any suspected misuse of telephones to their line manager or to the WBC Telecoms team.

13.4 Mobile Phones

13.4.1 WBC mobile phone users shall not loan or reallocate their phone or SIM card to anyone else without the prior knowledge and approval of the WBC Telecoms Team.

13.4.2 Mobile phone telephone usage is controlled i.e. users cannot dial premium rate or international number, and monitored to track call destinations, duration and costs.

13.4.3 Mobile phones are supplied with a 4-digit security PIN to prevent unauthorised usage. Users may change this PIN but should not divulge it to anyone else.

13.4.4 WBC mobile phone users should not let anyone use their mobile phone to make telephone calls (except other WBC users in special circumstances). Responsibility for calls made from an allocated phone rests with the nominated user and any misuse will also be their responsibility.

13.4.5 WBC staff shall not use their mobile phones whilst driving .

13.4.6 WBC staff shall not use their own mobile phones in work hours where this causes inconvenience or annoyance to colleagues or customers or where it provides a distraction or excessive loss of working time due to the making or receiving of telephone calls or text messages.

14. Use of Portable Equipment

14.1 All guidelines in this policy document apply equally to portable equipment as to fixed equipment. However portable equipment is more vulnerable to certain types of misuse, and to theft.

14.2 Portable equipment includes:-

- BlackBerry Smartphones
- Mobile Phones
- 3G Data Cards
- Personal Data Assistants (PDAs)
- Laptop PCs
- Tablet PCs
- Memory sticks
- Digital Cameras

14.3 Users issued with portable equipment should take all reasonable steps to safeguard the security and physical protection of these items by following the guidelines below:-

- When transporting portable equipment use approved protection e.g. laptop bag or backpack
- To prevent theft of portable equipment
  - — do not leave unattended
  - — do not leave visible in vehicles
  - — use locks e.g. Kensington Locks where possible
- Apply timeout password on any devices where these are available
- In the case of Laptop or Tablet PCs
  - — Only use WBC supplied equipment with an encrypted hard drive
  - — avoid saving data onto the local hard drive C: Drive
  - — attach the PC to the WBC network (at least once in every 4-week period) to ensure that it receives anti-virus updates
- If using memory sticks use approved password protected and encrypted devices, purchased through the ICT Help Desk
- Report thefts or suspected misuse immediately

15. Control of ICT Assets (Hardware and Software)

15.1 The ICT Service maintains an inventory of the Council's ICT hardware and software. Each ICT asset is recorded for the purposes of:-

- security protection
- insurance
- financial asset management
- health and safety
- equipment maintenance and replacement
- software licence compliance

15.2 No equipment or software should be acquired, disposed or relocated without the prior knowledge and approval of the IT Help Desk.

15.3 The ICT Service is responsible for maintaining the inventory and for providing current lists to Council Services of assets held.

15.4 Council Heads of Service are responsible for checking and verifying their asset holding against lists provided by the ICT Service, for informing the ICT Help Desk of any changes to the hardware or software holding and for ensuring their staff are using approved, licensed software. Heads of Service are also responsible for retrieving Council ICT equipment from staff when they leave and for informing the ICT Help Desk where any of these assets are reallocated.

16. Procurement of ICT Equipment and Software

16.1 All ICT equipment and software for use by or within WBC shall confirm to the technical standards laid out in the relevant appendix of the WBC ICT Strategy document.

16.2 Proposals to introduce new ICT equipment or software to the Council shall be controlled and will be evaluated for suitability by the Change Advisory Board (CAB) and may need to be introduced as part of a formal project, overseen by the Council's ICT Strategy Board.

16.3 ICT Systems and software should be ordered via the ICT Help Desk or in the case of large business system procurements by other means with the prior consent of the ICT Strategy Board. All ICT procurement is subject to the Council's procurement rules and processes.

17. Standards for Software Development

17.1 The development of software for use by or within WBC shall conform to the technical standards laid out in the relevant appendix of the WBC ICT Strategy.

17.2 Proposals to develop new software for the Council shall be controlled and introduced as part of a formal project, overseen by the Council's ICT Strategy Board.

17.3 Before engaging 3rd parties for the supply or development of new ICT systems users should liaise with ICT to seek advice and guidance.

17.4 Software developed in-house by non ICT staff e.g. access databases is subject to quality controls including:-

- Assurance on the competence of staff to conduct the work
- Standards for documenting the development
- Assurance that the developed software is supportable/sustainable if the developer were to leave the Council

To ensure these standards are complied with the ICT service does not ordinarily allow WBC users, outside of the ICT Service, to have software development tools, including Microsoft Access. Tools may be provided where service areas can demonstrate they meet the required criteria of development standards and responsibilities.

18. Monitoring the Use of ICT

18.1 Use of the Council communications equipment and systems (e.g. email, Internet usage, telephone usage) is routinely monitored by the Council for the following purposes:-

- to help ensure compliance with regulatory or self-regulatory practices and procedures
- To help ensure compliance with Information Security standards
- to ascertain or demonstrate achievement of operational quality standards
- to prevent or detect crime or misuse
- to detect and investigate unauthorised use
- to detect excessive use for personal purposes

Appendix A – Legal Acts Governing the Use of ICT

All users of WBC ICT Shall comply with all laws pertaining to the use of ICT. Current relevant law includes, but is not restricted to, the acts listed in the table below.

Legal Act
The Computer Misuse Act 1990
The Copyright, Designs and Patents Act 1988
The Data Protection Act 1998
The Defamation Act 1996
The Disability Discrimination Act 2005
The Equality Act 2010
The Freedom of Information Act 2000
The Human Rights Act 1998
The Obscene Publications Act 1964
The Protection of Children Act 1999
The Race Relations Act 2000
The Sex Discrimination Act 1975
The Telecommunications Act 1984
The Official Secrets Act 1911-1989 (Possible future requirement for some GCSx Users)

Appendix B – Glossary of Terms

Acronym	Meaning	Description
3G Data Card	3rd Generation Mobile Data Card	A small card that plugs into laptop or tablet PCs and allows internet access via the mobile phone network
GCSx	Government Connect Secure Extranet	A secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations.
ICT	Information and Communications Technology	Communication equipment and services to provide computing and telephony (often also known as IT)
SIM Card	Subscriber Identity Module	A small computer chip that fits inside a mobile phone and identifies the phone users id an personal facilities and details
PIN	Personal Identification Number	A 4-digit (usually) code which is used to control access to devices such as mobile phones
VoIP	Voice over IP	A technology which allows telephone calls to be made over data networks including the Internet
WAN	Wide Area Network	A computer or communications network that spans a wide geographic area of more than one building, town, or country