WREXHAM COUNTY BOROUGH COUNCIL

Corporate and Customer Services Department
ICT Service

ACCEPTABLE USE OF ICT FACILITIES

POLICY AND GUIDELINES

Revision	Date	Description
1.2	June 2016	Amended (Release)
1.21	November 2016	Review & Minor changes
2	February 2019	Final (Release)

CONTENTS

Page

1. INTRODUCTION AND SCOPE

1.1 This Acceptable Use Policy applies to all users of ICT (Information Communication Technology) facilities provided or supported by Wrexham County Borough Council.

ICT facilities include:

- Desktop and Mobile Computing facilities
- Telephony facilities (land-line and mobile)
- Controlled access to Wrexham's corporate network
- Controlled access to systems and data for business use
- Controlled access to the Internet and Intranet.
- Access to Wrexham's corporate e-mail system; and
- Any other approved ICT facilities.

Note for reciprocal and joint working arrangements with external organisations and partners, it can also include controlled access, via Wrexham's corporate network, to external networks, systems and data hosted at external locations such as other local authorities, NHS sites etc.

1.2 Definition of a User

1.2.1 A user is defined as any person who is provided with Wrexham County Borough Council ICT facilities either on a standalone basis or with access to the corporate network. This includes Wrexham members of staff, Councillors, temporary workers and contractors who have been assessed and approved for controlled access. **Note** - Work experience candidates or similar non-contracted individuals will not be provided with network access rights.

1.3 Document Structure

1.3.1 These guidelines are divided into **five** sections which set out:

i. Wrexham County Borough Council's policy statements for the acceptable use of ICT facilities, covering:

- General use of ICT facilities
- Procurement of ICT Hardware and Software
- Installation and use of ICT hardware - PCs, laptops, printers, mobile devices, telephones, scanners etc
- Installation and use of ICT software – system applications, databases, utilities [e.g. MS Office] etc.
- Data Security
- Agile Working (i.e. home and mobile working)
- Use of Mobile and Remote Computing Facilities
- Use of personally owned computer and removable media devices (e.g. laptops, mobile phones, PDA's, MP3 players etc.) – which is not permitted.

- Internet use
- E-mail use
- ICT Inventory and Disposal

ii. Users' responsibilities and what "Acceptable Use" of the facilities means.

iii. What monitoring will take place to confirm compliance with the policies

iv. What will happen in the event of non-compliance.

v. The main legal issues that the policies need to address.

NOTE – This policy has been reviewed and updated to take account of the Public Sector Network Code of Connection and the associated security standards.

1.3.2 Since 1st June 2005 all new Wrexham staff members joining the Authority have been required to sign the Terms and Conditions of Employment which includes a statement on acceptance of the *ACCEPTABLE USE OF ICT FACILITIES - POLICY AND GUIDELINES*.

1.3.3 Prior to the 1st June 2005 all other Wrexham ICT users at this time accepted the *ACCEPTABLE USE OF ICT FACILITIES - POLICY AND GUIDELINES* via an electronic acceptance process.

1.3.4 Other non-Wrexham employed users (for example, Councillors, contractors, non-Council staff working for the Authority, agency workers and staff from other public sector partner organisations), are required to read the guidelines and complete and sign Appendix C(1) and return it to The ICT Service, The Old Library, Queen's Square, Wrexham, LL11 1AT.

1.3.5 Members of staff who may be working on a temporary basis for Wrexham or those Wrexham staff members who have not previously signed up to the Acceptable Use Policy, are also required to read the guidelines and complete and sign Appendix C(1) and return it to the same address as stated in 1.3.4 above.

1.3.6 From time to time this policy document may need to be amended to ensure that policies on acceptable use remain relevant in the light of technological, legal or organisational developments. In such instances a copy of the revised policy will be published to the Intranet (SAM) and a global email will be sent providing a link to the revised policy. You should therefore periodically visit the Authority's Intranet site (SAM) to check for changes to the policy and guidelines.

1.3.7 Further to any future amendments (as stated in 1.3.6 above) if users wish to raise any objections or issues relating to those amendments then they may do so in writing to the ICT Lead. If users indicate a non-acceptance of this policy subsequent to any future amendments, then that user account on the network will be disabled and ICT facilities will not be reinstated until they agree to accept the policy.

1.3.8 Users should ensure that they are familiar with what is expected in the use of ICT facilities and with the policies governing their use. Failure to comply with the policies may result in disciplinary action.

1.3.9 If major changes are needed for any of the policies, the ICT Service will consult widely throughout the Authority and publicise the agreed changes to everyone concerned.

1.3.10 If there is anything in the guidelines that is unclear or if users have any questions about the policy, or if users have any questions or concerns about ICT monitoring, please contact the ICT Service.

1.4 Councillors Use of ICT Facilities

1.4.1 In addition to the acceptable uses described in this document, Members of the Council may use the Council's ICT facilities for the purposes of their roles as Members, as described in the Member Role Descriptions adopted by the Council.

1.4.2 For the avoidance of doubt, this includes use of the Internet by Members to access the websites of their political parties and those of local interest groups, and such other websites which Members may reasonably require access to in connection with their described roles. All use of ICT facilities is subject to the provisions of this policy document and guidelines. Copies of Member Role Descriptions are available from the Head of Corporate and Customer Services.

1.4.3 Councillors are not permitted to use Council ICT resources improperly for political purposes such as electioneering; for example the use of Council provided e-mail addresses as a correspondence address on a candidate's election literature would not be permissible as confirmed by the Ombudsman recently in his newly published Guidance to the Code of Conduct for Members. Such misuse could be found to be a breach of the Member Code of Conduct attracting one of the penalties under the Local Government Act 2000.

1.5 New Starters Account Request

1.5.1 New starters to the Authority have already signed their Terms and Conditions of Employment which includes a statement on acceptance of the *ACCEPTABLE USE OF ICT FACILITIES - POLICY AND GUIDELINES*. Prior to starting in post if managers' need to request a network login and email address for the new staff member they must complete the online form available in the Request Employee Joiner/Mover/Leaver section on the ICT Service Desk Portal.
Note – The request must be sent to ICT at least 7 working days prior to the new post starting date.

1.5.2 When requesting a new user account, managers must indicate whether the account is for a permanent staff member, temporary staff member or a non-employed user (for example, Councillors, contractors, agency workers or other non-Council users working with the Authority). Before an account is enabled for temporary staff members and non-employed users, the individual themselves **must** complete Appendix form C(1) and submit it to the ICT Service Desk.

2. POLICY STATEMENTS

2.1 General Use of ICT

2.1.1 Wrexham County Borough Council provides ICT facilities to promote effective communication relating to its business. The Council provides these facilities on the basis that:

- Staff members have already accepted this policy document (As stated in 1.3.2 and 1.3.3)
- Users read, understand and abide by the policy statements contained within this document.
- New members of staff will be required to sign the Terms and Conditions of Employment which include a statement on the acceptance of the *ACCEPTABLE USE OF ICT FACILITIES - POLICY AND GUIDELINES*
- Temporary staff, or permanent staff who have not previously signed the AUP and non-employed users (for example, Councillors, contractors, agency workers or other non-Council users working with the Authority), must complete Appendix C(1) and submit it to the ICT Service Desk.
- Where a Wrexham department requests a business e-mail address to be used as a service contact point, e.g. planning@wrexham.gov.uk, Appendix C(2) must be completed, signed and returned. A named individual must be responsible for monitoring the e-mail account to ensure that all messages received are dealt with promptly and that e- mails are deleted or archived once they have been dealt with.

  Note - The use of generic non-assigned (proxy) network login user accounts (i.e. where a named user is not defined) is not permitted.

2.1.2 Wrexham County Borough Council will ensure that its ICT facilities are protected so that it can continue to operate its business. (See the ICT Security Policy on the Authority's Intranet site - SAM).

2.1.3 Users should do nothing to endanger the security or integrity of the Authority's systems. External files including those:

- received as e-mail attachments;
- downloaded from the Internet;
- received on disk or other computer media,
- on USB memory sticks; or
- received via any other data storage device

can introduce malicious software, such as computer viruses, that can damage the Authority's systems and networks.

2.1.4 Users should immediately contact the ICT Service Desk on 01978 29 2340 if they suspect that an external file contains a virus. Suspect files must not be opened, uploaded or distributed until the ICT Service has completed its investigation. For further guidance on the use of removable media see section 2.5 on Data Security.

2.1.5 Line managers are responsible for ensuring that proper use is made of official time. ICT facilities are provided for business use with the only exception being the limited personal use of email and internet as described in sections 2.9.3 and 2.10.14.

2.1.6 All ICT activity is monitored for appropriate use - see section 4**.**

2.2 Procurement for ICT Hardware and Software

2.2.1 All ICT hardware for use within Wrexham **must** be procured by the ICT service following the Authority's Procurement Policy.

2.2.2 Unless otherwise authorised by the ICT Service, all ICT software for use within Wrexham **must** be procured and installed by the ICT service in line with the Authority's Procurement Policy. Consideration should always be given to the need to carry out a Privacy Impact Assessment when purchasing new software.

2.3 Installation and Use of ICT Hardware

2.3.1 ICT Hardware, e.g. PCs, laptops, PDAs, scanners, digital cameras, printers, telephones, mobile phones etc., provided by Wrexham County Borough Council **must only** be used for work purposes relating to the Authority's business. The exceptions to this are the limited personal use of e-mail and internet as described in sections 2.9.3 & 2.10.14.

2.3.2 Unless otherwise agreed by the ICT Service, ICT hardware is only to be installed by staff from the ICT Service.

2.3.3 The use of personally owned ICT equipment, e.g. laptops, mobile phones, PDA's, MP3 players, wireless capable devices, USB memory sticks etc., to connect, upload or download data on Wrexham's network is not permitted. Attempting to use such devices on Wrexham's network will be logged and prevented by the Authority's Endpoint Security Software – See Section 2.5 on Data Security.

2.4 Installation and Use of ICT Software

2.4.1 ICT software provided by Wrexham County Borough Council, i.e. MS Office, databases, graphic and design packages etc., **must** only be used for work purposes relating to the Authority's business.

2.4.2 Software upgrades provided by vendors for existing applications should only be loaded with the prior agreement and involvement of the ICT Service.

2.4.3 All desktop software is to be installed by ICT Service staff unless otherwise agreed by the ICT Service.

2.4.4 It is **not** permitted for users to load personal or non-business related software or files on to any Council owned ICT equipment. The loading of such software or files may result in disciplinary action. This would include downloading software from the internet.

2.4.5 Loading unauthorised software (which has not been approved by the ICT Service) can expose the Authority to malicious software and cause damage to computer operating systems and the wider network.

2.4.6 It is also prohibited for staff to recklessly access or transmit information about, or software designed for, breaching security controls or for creating computer viruses or other malicious software.

2.4.7 All staff are responsible for ensuring that they act with due care and vigilance in respect of protecting the Authority's ICT assets from malicious software, such as viruses.

2.4.8 Any employee who suspects that their work station may have been infected with malicious software must immediately contact the ICT Service Desk on 01978 29 2340. Users must switch off their work station and leave it powered off until advised by a member of the ICT Service.

2.5 Data Security

2.5.1 In carrying out the functions of a Local Authority, Wrexham is often required to hold certain personal and/or sensitive information relating to service users, staff, businesses, partner organisations or information relating to Council business. As the custodians of this information it is critical that we maintain high levels of data security at all times to ensure it remains safe and secure.

2.5.2 Wrexham County Borough Council has a duty to ensure personal data is managed in accordance with the Data Protection Act. This includes complying with Principal 7 of the Act which states that '*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'*

2.5.3 All staff must be aware of the requirements of the Data Protection Act. Further guidance on the requirements of the DPA and details of the mandatory training which must be completed are also available on the Intranet – SAM.

2.5.4 As a minimum, when staff are away from their desks for extended periods of time they should ensure that access to their computer / data is prevented by

using the Ctrl-Alt-Delete command to lock their PC. Computer screens near windows or in public areas should be positioned so they cannot be viewed by unauthorised personnel.

2.5.5 The Authority utilises Endpoint Security software to prevent the inappropriate downloading of Council data and to control data leakage. This software also prevents the introduction of malicious software. It controls which devices are permitted access to Wrexham's network and will prevent any non-approved devices, such as USB sticks, hard drives etc. or any other device capable of storing data from working on Council equipment. It can also limit the use of recordable CDRW / DVDRW drives which are present in the Council's PCs and laptops.

Within this software the ICT Service has the ability to 'white-list' any genuine Wrexham devices to permit their use on the Councils network. For further details on this process either contact the ICT Service or your departmental ICT Liaison officer.

Personally Owned Devices

2.5.6 It is not permitted for any personal devices, capable of storing data, to be connected to the corporate network or to any council owned equipment. The use of such devices may result in disciplinary action being taken. This would include, but is not limited to, the use of personally owned MP3 players, cameras, phones, mobile devices, laptops or any other personal device capable of storing or viewing data.

The Authority's Endpoint Security software will prevent the use of such personally owned devices and will log any such inappropriate activity.

Note – The ICT Service is looking at future 'bring your own device' (BYOD) options for staff which may compliment existing working practices. The use of such devices will only be permitted where there is a particular business case for doing so and where it can demonstrably bring benefit to the service.

Data Storage

USB Memory Sticks (Also known as Flash Drives or Pen Drives)

2.5.7 Wherever possible the use of removable media should be avoided, and on no account should employees use any personally owned removable media or computer device to try and download Council data, connect to the corporate network or to council owned computer equipment. The Authority's Endpoint Security software will prevent the use of such devices and log such occurrences.

2.5.8 In instances where the use of USB memory sticks cannot be avoided, only those supplied by the ICT Service are permitted to be used within Wrexham for the storage of Wrexham County Borough Council data. The ICT Service issues USB sticks with Wrexham's corporate logo on them as a visual means

of checking that staff are complying with this requirement. These approved Wrexham devices will be permitted access through the Endpoint Security software.

2.5.9 The USB memory sticks provided by the ICT Service are fully encrypted with enforced password protection. These devices protect the data on them through the use of strong encryption software and can only be accessed by secure password. These USB memory sticks can be purchased by emailing Corporate ICT Procurement and supplying your cost code.

Note – If a user forgets the password on these devices then the protection software will automatically re-format the USB memory stick. This is an inbuilt protection mechanism which renders the data on the device irretrievable if it is lost or stolen.

2.5.10 Memory sticks purchased from the ICT Service before May 2008 did have password protection software which was activated by the user, however these devices were not encrypted. The use of these devices is not permitted. Users with these devices must return them to the ICT Service and if deemed required, arrange for a replacement, encrypted versions along with a cost code. For further advice contact the ICT Service.

Data Storage on Other Removable Media

2.5.11 Wherever possible the use of other removable media should be avoided, this would include the use of removable CDs/DVDs, external hard drives, media cards as used in phones, digital cameras, mobile devices etc.

DVD's, CD's & Floppy Disks

2.5.12 As encryption software cannot be easily applied to DVD's and CD's they should never be used to store personal or sensitive information / data. Similarly floppy disks, although an older technology, must never be used to store personal or sensitive information. The use of CDRW/ DVDRW devices on PCs and laptop will be controlled using the Authority's Endpoint Security software.

External Hard Drives

2.5.13 External hard drives will not be purchased for use within departments unless there is a specific business case for doing so and this has been approved by the ICT Service. Where they are required for business use to store Council information / data, encryption software will also be installed to ensure data security.

Media Cards

2.5.14 Media cards, such as those used in digital cameras and mobile phones, are only permitted to be used for defined business reasons where this has been approved by the ICT Service. Such devices must not to be connected to any

Council ICT equipment unless otherwise agreed by the ICT Service. They must not be used to store any personal or sensitive data.

Note - Any approved portable device used to store Council data must be erased once the work activity requiring the storage is completed.

Secure Data Transfer

2.5.15 Departments within the Council are sometimes required to share information with authorised external partners, suppliers or individuals. If there is a requirement to send personal or sensitive information / data between other external organisations or individuals, then reference must be made to Wrexham's Secure Data Transfer Standards and Procedures. Where appropriate, information sharing protocols must also be in place, in line with the Wales Accord for the Sharing of Personal Information (WASPI), also available on the Intranet – SAM.

Note

The Secure Data Transfer Standards and Procedures does not specifically cover the internal transfer of information / data between service areas or individuals within Wrexham County Borough Council, however similar principals should be applied.

2.5.16 The Secure Data Transfer Standards and Procedures are in place to ensure appropriate procedures are followed when transferring personal and/or sensitive information / data in electronic or printed formats. This would include transfer of information by e-mail, fax, post, the physical handover of information and by automated electronic transfer processes, such as FTP.

2.5.17 No personal and/or sensitive information and data is to be sent out of the organisation without prior approval from the relevant Head of Department and with agreement from the ICT Lead on behalf of the Head of Corporate and Customer Services. If transfer is agreed then the recipients must sign a non-disclosure agreement and confirm their data care arrangements, including the future data destruction or return requirements.

2.5.18 Much of the information held by the Council should be classed as potentially sensitive and therefore the requirements of the Secure Data Transfer Standards and Procedures must be considered at all times.

2.5.19 A list of all data transfer requests received will be maintained by the ICT Service for reference.

2.5.20 The requirements of the Secure Data Transfer Standards and Procedures are in accordance the Council's statutory requirement to comply with the Data Protection Act.

2.5.21 All staff should make themselves aware of this requirement of the Secure Data Transfer Standards and Procedures document and failure to comply

may result in disciplinary action. A copy of the document is available on the Intranet - SAM.

Government Connect Code of Connection

2.5.22 As part of the Public Sector Network (PSN) programme and the Code of Connection (CoCo) to which Wrexham subscribes, we are required to ensure significant security measures are in place when permitting remote access to the corporate network by external suppliers.

2.5.23 The ICT Service has developed a Wrexham CBC 'Code of Connection' document to which all external suppliers have to sign prior to being permitted remote access. Wrexham's Code of Connect document ensures suppliers adhere to the strict security standards set, which includes only permitting remote access to corporate systems using secure Citrix technology. The ICT Service will manage this process with suppliers.

Loss of ICT Devices & Data

2.5.24 It is the duty of all users to immediately report any actual or suspected breaches in information security to their own line manager and the ICT Service.

2.5.25 If a Council device is lost or stolen then it must be reported immediately to the ICT Service (this would include the loss of USB memory sticks).

2.5.26 Full details of the equipment and any potential data loss must be provided so that the implications of the loss can immediately be assessed. If the device has been stolen it may also be necessary to contact North Wales Police to report the incident. This should be determined by discussion with the ICT Service.

Misuse of Data

2.5.27 If users are concerned that Council information / data is being used inappropriately then they must contact the ICT Service and inform their line manager who will follow the Data Security Breach Management Procedures available on the Intranet – SAM.

2.5.28 If, for whatever reason staff feel that they cannot raise the issue with their line manager, then they should bring it to the attention of someone more senior either within or outside of their own department. An internal list of potential contacts is available on the Council's Whistleblowing Policy intranet page. If staff require confidential advice first, they can also contact Public Concern at Work on 020 7404 6609.

2.5.29 For further information on reporting inappropriate work practices within Wrexham, advice and guidance is available in the Council's Whistleblowing Policy on the Intranet – SAM.

Data Encryption on Mobile Devices

2.5.30 With the increasing use of mobile devices such as laptops, tablets and slate devices, within Wrexham, it is important that adequate steps are taken to safeguard the data / information saved upon them in case they are lost or stolen.

2.5.31 Safeguarding this information can be achieved through the use of strong encryption software which encrypts data files on the device to internationally recognised standards. This therefore ensures that if the device were lost or stolen then the data / information will be irretrievable.

2.5.32 All new laptops purchased by the ICT Service after the 1st August 2010 will come with mandatory encryption software already installed. Where appropriate any inbuilt encryption technology which comes as a ready option on devices such as tablets, slates etc. will be activated prior to them being provided to users.

2.5.33 The ICT Service is also undertaking a retrospective task to install encryption software on existing corporate laptops. An assessment of the mobile devices within Wrexham has been undertaken and 'high risk' devices such as those likely to contain personal / sensitive information will be given priority.

2.5.34 Where smart phones or other mobile devices are in use, the in-built password protection facilities must be activated on these devices as a minimum requirement. However, if the devices are used to store information / data which could be considered personal and/or sensitive, then users must seek advice from the ICT Service regarding the installation of encryption software.

2.6 Agile Working

2.6.1 If there is an approved business case for users to access corporate systems from remote or home working locations the ICT Service can facilitate this through the use of secure Citrix technology. Initial agile working business requests should be made by contacting the Performance, Improvement & Partnerships team. This technology can also provide users with access from designated 'hot desk' areas which will further compliment agile working arrangements in line with Wrexham's corporate plans for agile working.

2.6.2 Guidelines on providing 'Remote Access to Corporate I.T. Systems' will be then be forwarded to the requesting department. This document outlines what is permitted in terms of secure remote access to corporate systems as well as providing guidance on potential equipment and licensing requirements.

2.6.2 After considering the requirements set out in the 'Remote Access to Corporate I.T. Systems' document, departments are expected to provide a business case to accompany the formal request. This business case should provide justification for request and also provide any further details which

have been requested by the ICT Service. The business case and any other relevant documentation must be counter signed and approved by the respective departmental Head of Service prior to being sent to the Corporate Gateway for senior approval before being sent to supporting services for comment.

2.7 Use of Mobile and Remote Computing Facilities

2.7.1 Wrexham County Borough Council recognises that mobile computing facilities provide a valuable business benefit to the Authority. This includes provision of Authority supplied laptops, smart phones and any other handheld computers or mobile device. It can also include any facilities for remotely accessing the corporate network via Citrix home working initiatives.

2.7.2 Any user provided with mobile computing facilities **must**:

- upon receiving a device sign an acceptance form to ensure that they adhere to the conditions stated below
- use them responsibly and comply with all relevant policies and procedures as if they were using the systems in their normal place of work
- take appropriate measures to ensure the physical protection of equipment from loss, theft, damage etc.
- ensure that any password protection software is activated and that passwords are always kept secure
- regularly transfer critical files and data to the Authority's network by secure means, so that the data can be backed up routinely
- return the equipment to the ICT Service when requested to do so for routine maintenance or any other purpose
- ensure that any Citrix authentication devices provided to allow secure remote access to the corporate network are always used appropriately and only by them as the authorised user.
- report any loss or theft of devices immediately by following the procedure set out in sections 2.5.24 to 2.5.25.

2.7.3 In addition any user provided with mobile computing facilities **must not**:

- use the equipment for any private use at any time, other than those permitted personal uses mentioned in section 2.9.3 and 2.10.14.
- store files which contain personal and/or sensitive information on the device unless adequate password and encryption protection has been put in place.
- download files from the Internet to Authority supplied equipment.

- install unauthorised software, e.g. games or screensavers etc., onto Authority supplied laptops, handheld devices, PCs or any other related equipment.
- leave the equipment unattended, even for a few minutes, particularly when travelling away from the office or attending events.
- take corporate equipment, including laptops, mobile devices, cellular telephones etc. aboard without specific approval of the relevant Head of Service and the ICT Lead on behalf Head of Corporate and Customer Services.

2.8 Use of Personally Owned Computer Devices

2.8.1 With regard to ICT devices owned personally by users which are not supplied by the Authority, this includes laptops, smartphones, MP3 players, digital cameras, USB memory sticks or any other electronic device; users **must not**:

- Connect such devices to the Council network (whether remotely or on-site), for any purpose unless with the express permission of the ICT Lead on behalf of the Head of Corporate and Customer Services Department.
- Use their own mobile devices to store (download or upload) any organisational information without the express permission of the ICT Lead on behalf of the Head of Corporate and Customer Services Department. The Authority's Endpoint Security software will prevent the use of such devices and log such occurrences.

2.8.2 Systems are in place to monitor compliance with the above and any non-compliance may result in disciplinary action. See section 2.5 on Data Security.

2.9 Internet Use Policy

Users should cross reference to section 3 on User Responsibilities when reading this section

2.9.1 Wrexham County Borough Council recognises that access to the Internet is a valuable tool and can provide significant benefits for many of our business requirements.

2.9.2 Users may access the Internet during normal working hours for work related business only.

2.9.3 Personal use of the Internet is permitted on the following basis.

- Users access the internet on their own time whilst they are 'clocked out' or on official breaks during their normal working day.

- Users will not be allowed to operate any private business at any time through the use of the Authority's facilities and must conduct themselves in accordance with the Council's Officer Code of Conduct.
- Access to social networking sites will not be permitted. **Note** – Also see section 2.11 on Social Networking for further information and exceptions.
- The Authority's web content filtering will remain in place at all times for security reasons and to prevent the possibility of reputational damage by misuse – see section 2.9.5.
- The personal use of the internet is provided on the basis of trust and managers will have responsibility for monitoring that users are following these conditions of access. It should be noted that as part of Wrexham's standard security procedures all internet activity is logged against individual users so that the Council maintains a record of the sites visited and the time spent on each website. This information could be useful in helping identify any misuse of the internet.

2.9.4 Access to the Internet is provided by the Authority's link to Wales' Public Sector Broadband Network. Usage of the network is governed by a connection agreement which stipulates that the Authority is liable for any breaches of the terms of the agreement by end users, including staff, Council Members or any other user provided with access. Therefore all users must comply with the terms set out in section 5 of this policy relating to Legal Issues when using Internet facilities.

Internet Web Filtering

2.9.5 Access to the Internet from Wrexham's network is 'filtered' using a web-filtering system. This system monitors all web access and classifies web sites depending on the subject and information present. The system can therefore prevent access to certain types of 'inappropriate' web sites.

2.9.6 If users are aware that a web site is blocked when access is actually required for valid business reasons, then the Request to unblock website is required to be completed via the ICT Self Service Portal.

2.9.7 Any use of the Authority's ICT systems to publish, distribute, or try to gain access to obscene, discriminatory, pornographic, extremist or excessively violent material will lead to disciplinary action being taken – see section 5.10.

2.10 Use of E-mail Policy

Users should cross reference to section 3 on User Responsibilities when reading this section

External E-mail

2.10.1 When conducting Council business via email, users are must always use their Council email address (name@wrexham.gov.uk). No other email address is to be used for conducting Council business.

2.10.2 If there is a requirement to send personal and/or sensitive information via e-mail then the information must be encrypted prior to being sent. In all such instances reference must be made to the 'Secure Data Transfer Standards and Procedures' which provides guidance on appropriate data transfer mechanisms. This policy is available on SAM and further advice and guidance is available by contacting the ICT Service.

2.10.3 For all general external correspondence, i.e. that which does not contain personal and/or sensitive information or data, e-mail may be used as appropriate.

2.10.4 When using email, if there is a requirement to restrict access to the recipient (s) this should be clearly stated in the subject line of the email. Reference must also be made if the email / content should not be forwarded or shared to another recipient. Before sending the email, ensure that the email address of the recipient (s) is correct.

2.10.5 Correspondence dealing with contractual, financial, legal or confidential issues of the Authority can be sent via email providing that it complies with the requirements of the 'Secure Data Transfer Standards and Procedures'. However, contracts or documents which require an actual signature should be sent by recorded post on Council letter headed stationery.

For personal and/or sensitive information, see 2.5.15 Secure Data Transfer.

2.10.6 Some employees are required to send personal and/or sensitive data to external public and private sector organisations who work with the Council to deliver services. Refer to section 2.5.15

2.10.7 To protect potentially personal and/or sensitive information which is received:

- via e-mails from external organisations and individuals; or
- from other internal e-mail users within Wrexham

the setting of rules to auto-forward e-mails to external e-mail accounts is not permitted.

2.10.8 Users should not forward any email which advises the recipient of a virus warning or similar threats as the information may be inaccurate, a hoax or scam email. If there is a requirement to inform users of a specific threat from malicious software, then the ICT Service will make users aware by issuing an email bulletin or providing information on the intranet. If you receive any such emails from external sources, do not forward them and contact the ICT Service for advice.

2.10.9 Use of the corporate email facilitates must be used in line with the **Code of Conduct** and must not be used for personal or political campaigns. Paragraph 9.4 of the **Code of Conduct** states:

"Qualifying employees of relevant authorities must ensure that they use public funds entrusted to them in a responsible and lawful manner and **must not utilise property, vehicles or other facilities of the Authority for personal use unless authorised to do so."**

2.10.10 All external e-mails will automatically include the Authority's standard bilingual disclaimer statement, the text of which is shown in Appendix A.

2.10.11 Users should not open any file attached to an external e-mail unless they were expecting to receive it from a known source. If the origin of a file is unknown, **DO NOT** open or distribute it. Contact the ICT Service Desk on 01978 29 2340 for guidance.

2.10.12 Users who are responsible for monitoring generic departmental e-mail addresses for public use, e.g. planning@wrexham.gov.uk, must respond to any correspondence received in line with the time scales set in the Communications and Brand Identity Toolkit. Further guidance is provided in the Communications and Brand Identity Toolkit document, available on the Intranet – SAM.

Internal E-mail

2.10.13 E-mail is acceptable as a standard form of internal communication except for correspondence:

- that requires an actual signature of a Director or Head of Department – this should be sent by memo;
- that is marked personal or confidential, or which contains sensitive, personal information relating to an individual, identifiable person. In all such instances reference must be made to the principles set out in the Secure Data Transfer Standards and Procedure – available on the Intranet – SAM.

Note - If there is a requirement to restrict access to the recipient only for any other reason then this should be clearly mentioned in the text of the email. It should also outline that the content of the email should not be forwarded or shared.

Personal Use of E-mail

2.10.14 E-mail facilities may be used to send personal messages provided this does not impinge upon its use for official purposes ***and is confined to outside working hours (i.e. when the user is clocked out or on an official break during their normal working day).***

2.10.15 To ensure privacy, users should include the word “Personal” in the subject line of any personal messages. E-mails marked “Personal” will be subject to normal monitoring but will not be opened for monitoring purposes unless there are exceptional circumstances, for example when serious crime is suspected.

2.10.16 All of Wrexham’s e-mail facilities are monitored. If it is discovered that e-mails are being sent which contain defamatory, extremist, obscene discriminatory, libelous, offensive or harassing content; or contain any other attachments or content which may be considered inappropriate or illegal, then disciplinary and/or legal action may be taken against those concerned.

2.11 Social Networking Sites

2.11.1 The widespread use of social networking sites has given Wrexham County Borough Council the opportunity to communicate with audiences in new ways. Recently this has included providing access to our website content via Facebook and Twitter. The management and update of these facilities are undertaken solely by Wrexham’s Communications Section. For further information contact Wrexham’s Communications Manager.

2.11.2 In all other instances access to social networking sites through Wrexham’s network is blocked, unless specifically authorised by a Head of Department and the ICT Lead for valid departmental functions.

2.11.3 The inappropriate use of social networking sites by staff is governed under Wrexham’s Corporate Code of Conduct and the Disciplinary and Capability Policy and Procedures.

2.12 Departmental ICT Inventory

Equipment Moves and Changes

2.12.1 ICT equipment within departments should not be moved or reassigned to another user without the prior knowledge and agreement of the ICT Service.

2.12.2 The ICT Service will require at least 1 months’ notice for any new staff so that equipment can be assigned correctly within the inventory or ordered if required. Equally when a member of staff leaves the organisation the ICT Service must be informed immediately.

Redundant ICT Equipment

2.12.3 When ICT equipment is updated within departments, the older equipment which is being replaced must be returned to the ICT Service for reuse or disposal. No obsolete ICT equipment is to be retained by departments after a replacement has been issued.

2.12.4 Any other ICT equipment which is either no longer working, obsolete or no longer required must be returned to the ICT Service for reuse or disposal. This would include PC's, laptops, mobile devices, telephones, data storage devices (such as USB sticks, external hard drives etc.), digital cameras or any other associated ICT equipment.

ICT Inventory Audits

2.12.5 To ensure that an accurate inventory of ICT equipment is maintained at all times, the ICT Service will, on an annual basis, require departments to participate in an audit exercise. Each year departments will be provided with a list of their current ICT equipment from the inventory and they will be asked to check and verify that it is correct.

2.12.6 The completion of this audit is a requirement placed on all Heads of Department under Wrexham's Financial Regulation 21.16 which states that :

'*Asset records and inventories are to be checked by Heads of Department annually to ensure: (a) that new items are entered, (b) that items are present and (c) any deficiencies are either accounted for or investigated without delay'*

2.12.7 The ICT Service will initiate this process and coordinate with the Heads of Department and ICT Liaison Officers as required. Departments will be expected to carry out the audit and return the documentation to the ICT Service on a timely basis.

2.13 Energy Saving / Carbon Reduction

2.13.1 The ICT Service ensures that all ICT equipment purchased is compliant with current EU energy saving ratings. In response to the Corporate carbon reduction programme, the ICT Service works to implement new technologies which will assist in reducing Corporate energy consumption relating to ICT equipment, e.g. desktop power management software.

2.13.2 All users of Wrexham's ICT equipment can assist in this process by ensuring that they switch off their PC, monitor, or any other device at the end of each day, or when they are away from their desk for extended periods of time. Users are also reminded that for security purposes the Ctrl, Alt, Delete command should always be used to lock their PC when away from their desk for extended periods of time.

3. USERS' RESPONSIBILITIES

3.1 General

3.1.1 ***Users are responsible for ensuring that they do***:

- Understand and abide by all the policy statements contained within this document. For the avoidance of doubt, users are required to fully comply with all policy statements shown in section 2.
- Comply with the policies and the underlying laws shown in section 5, e.g. Computer Misuse Act 1990, Data Protection Act 1998 etc.
- Use the ICT facilities provided for work purposes only; the only exceptions being:
    - *The limited personal use of e-mail and the internet*

  (providing this is done outside working hours or on an official break during their normal working day).
- Use the Ctrl, Alt, Delete command to lock their PC when away from their desk for extended periods of time.
- Ensure screens are positioned so that data is not visible by unauthorised personnel.
- Use the Internet in a responsible way and within the terms of the AUP

3.1.2 ***Users are responsible for ensuring that they do not***:

- Attempt to use the ICT facilities for any unauthorised purpose.
- Misuse or damage any Council ICT facilities.
- Load / download unauthorised software or files onto any of the Authority's PCs, laptops or any other Council owned ICT equipment.
- Allow external organisations to connect their ICT equipment to the Authority's network.
- Divulge their passwords to anyone else or leave their passwords visible on a piece of paper or Post-it note etc., left on or near their monitor.
- Visit Internet sites that are offensive or illegal.

3.2 Use of ICT facilities – Email

3.2.1 ***In addition to compliance with the general requirements shown in 3.1 above, when using e-mail, users must ensure that they do not:***

- send sensitive or confidential information by e-mail - unless otherwise in accordance with the processes outlined in the Secure Data Transfer Standards and Procedures – see sections 2.5.15 to 2.5.21.
- use offensive, harassing or discriminatory language; (Jokes or comments that may seem innocent to one person can cause serious offence to another). The Authority has strict rules governing equality, discrimination and harassment that, when applied, can lead to staff disciplinary proceedings. In addition, the Authority's reputation can be

affected, and it can become liable to legal action, where such e-mails travel outside the office with the Authority's domain name (wrexham.gov.uk) on it;

- send threatening, intimidating or libelous messages; (*Users may be exposed to a potential legal liability that affects them as individuals, their line management and the Authority)*
- enter into a contract on behalf of the Authority; or

3.2.2 Use of ICT facilities – Internet

In addition to compliance with the general requirements shown in 3.1, when using the Internet, users must ensure that they do not:

- Access web sites which are not work related in work time. **Note** Personal use of the internet is permitted providing that it complies with the conditions shown in section 2.9.3.
- Download software or files from the Internet without the permission of the ICT Service.
- Upload information or data to the internet.

3.3 Who to Contact

3.3.1 The ICT Service has introduced a Self Service Portal that helps users with issues and requests. Users are asked to use the portal in the first instance as the operators may be busy and the portal can automatically log your request.

3.3.2 To make the most of the ICT facilities, users should contact their Manager or departmental MIS / ICT Coordinator:

- For all ICT training needs (if you don't know how to do it, then ask)
- For requests for non-standard ICT software (your manager should then contact the ICT Service Desk).
- To report any suspected misuse of the Authority's ICT facilities or information / data.

The ICT Service Desk (Self Service Portal, email ictservicedesk or telephone 01978 29 2340) should be contacted **immediately** for any:

- Problems with the ICT facilities
- Accidental damage to the ICT facilities
- Viruses or suspicious files or attachments received in e-mails.
- Reporting lost or stolen ICT equipment.
- Requesting any ICT equipment moves or changes.
- Or any other issue outlined in this policy document

Computer audit (e-mail or telephone 01978 29 2771) should be contacted **immediately** for any:

- "ICT incidents", for example if you find evidence of pornography; hacking or deliberate misuse of ICT equipment;
- Inappropriate Internet sites visited accidentally.
- To report any other issues of misuse.

Note

If an offensive site "pops-up" unexpectedly, try to close it down by clicking on the "x" box in the top right-hand corner. If there is no "x" box, do **not** click on any other options available and contact the ICT Service Desk on 01978 29 2340 immediately. Users must switch off their work station and leave it powered off until advised by a member of the ICT Service.

4. MONITORING

4.1 General

4.1.1 In line with the Lawful Business Practice Regulations 2000, these guidelines make it clear that all ICT activity in Wrexham County Borough Council is subject to monitoring. Monitoring takes place to protect the Authority's ICT facilities and reputation, and to confirm compliance with the relevant legislation and Wrexham County Borough Council's ICT policies.

4.1.2 All users must give their formal consent to the Authority monitoring their ICT activity. Wrexham County Borough Council's staff do this by accepting this policy document under their terms and conditions of employment or by previously accepting this policy as stated in section 1.3.2 and 1.3.3. Other non-Wrexham County Borough Council staff, temporary staff or Wrexham staff who have not previously signed up to the Acceptable Use Policy do this by completing and signing the Statement of Agreement in Appendix C(1) as stated in section 1.3.4 and 1.3.5.

4.1.3 Much of the Authority's monitoring is carried out automatically:

- The firewall detects e-mails containing malicious files, such as viruses
- E-mails are automatically screened for appropriateness and security. This monitoring is based on sets of rules, for example file attachment types to be quarantined or "sensitive words" to be quarantined or deleted. These sets of rules are regularly reviewed and updated to deal with emerging threats.
- All Internet activity is logged automatically to provide statistical information
- All websites are automatically screened to ensure that they are appropriate. Access to inappropriate websites is prevented.
- All telephone activity is logged automatically for billing purposes.
- Certain Council telephone numbers also have automated voice recording for training & verification purposes.

4.1.4 The ICT Service carries out monitoring in order to protect the Authority's network and computer systems and to confirm compliance with legal requirements and the Authority's policies.

4.2 Non-compliance

4.2.1 If the monitoring in 4.1.1 – 4.1.4 above identifies ***evidence of misuse of the ICT facilities*** this may lead to disciplinary action, up to and including dismissal.

4.2.2 If the monitoring in 4.1.1 – 4.1.4 above identifies ***evidence of possible criminal activity*** this may be passed on to the police.

4.2.3 As a user you have a responsibility to report any misuse of the Authority's

ICT facilities to either your line manager, the ICT Lead or the Audit and Technical Manager.

5. LEGAL ISSUES

5.1 General

Providing employees with access to ICT facilities is expected in today's modern working environment. However, misuse of these facilities by employees could have serious legal implications for the employees concerned (see below) and for Wrexham County Borough Council as a result of vicarious liability, which is explained in more detail in Appendix A.

5.2 Data Protection

The Authority holds a wealth of confidential information relating to its staff, customers, clients and suppliers, much of which is in electronic format. The unauthorised release of such information, for example via e-mail, would be in breach of the General Data Protection Regulation (GDPR) and could make individual employees and the Authority liable to substantial fines. Guidance on the Data Protection Act is available on the Intranet – SAM. Staff must ensure they complete the mandatory Data Protection training, along with mandatory annual refresher training.

5.3 Freedom of Information

The Freedom of Information Act 2000 ("the Act") is fully in force from the 1 January 2005. The aim of the Act is to make public bodies more open and accountable by creating a right for any person to request any information held by them (subject to exemptions). As a public body, the Council is subject to the Act and is committed to complying with it. Employees should familiarise themselves with the Council's policy on Freedom of Information – a copy is available on the Intranet – SAM and staff must ensure they complete the mandatory Freedom of Information training.

5.4 Human Rights

The Human Rights Act 1998 gives individuals the right to respect for private and family life, home and correspondence. By encouraging users to identify e-mails as "personal" in the subject heading, the Authority is looking to safeguard the privacy of employees' correspondence. E-mails marked "Personal" will be opened for monitoring purposes only in exceptional circumstances, for example, where serious crime is suspected. They will however, still be subject to the normal monitoring described in section 4.

5.5 Harassment, Discrimination and Defamation

If employees transmit obscene or discriminatory materials or harass other individuals by e-mail, this may cause offence and incur liability for the individuals concerned, as well as for the Authority. Similarly, if employees use the ICT facilities to make defamatory or discriminatory statements they (and the Authority) could face legal action. Users should make themselves aware of the contents of the Equality Act 2010 and other UK legislation and regulations covering issues of age, disability, race, religion or belief, sex, sexual

orientation and any other 'protected characteristic' as defined in the Equality Act 2010. The HMSO website contains full details of this legislation.

5.6 Equality Legislation

Wrexham County Borough Council is committed to preventing the use of its computer systems and networks for the distribution, publication or viewing of material which would be considered discriminatory. This would include discrimination on the basis of age, disability, race, religion or belief, sex, sexual orientation or any another 'protected characteristic' as described in the Equality Act 2010.

5.7 Software Licensing and Copyright

Only software that is developed by the Authority or licensed or provided by the developer to the Authority should be used on Wrexham County Borough Council's ICT facilities. Under no circumstances should users copy software from one PC to another without the appropriate licence agreement. The Authority could be liable to substantial fines if it was discovered using software without the appropriate licence. Appendix B explains how to obtain business related software for use with Wrexham County Borough Council.

Users should take care in copying material obtained through attachments to e-mails or, from information sources via the Internet. There may be copyright or other restrictions on such material (often identified by ©, ™ or ®) and unauthorised use including copying or onward transmission may be an infringement of copyright (section 17, Copyright, Designs and Patents Act 1988).

5.8 Computer Misuse

The Computer Misuse Act 1990 makes it illegal to gain unauthorised access to a computer system (hacking), to extract data from the system (confidentiality) or to amend the system without permission (including introducing viruses). The Authority has a duty to put procedures in place to prevent unauthorised access. If the Authority fails to do this it is likely to be in breach of the Data Protection legislation and could be liable to substantial fines.

5.9 RIPA, the Lawful Business Practices Regulations and Employment Practices Data Protection Code: Monitoring at Work

The Regulation of Investigatory Powers Act 2000 (RIPA) states that the interception of communications in the course of transmission without consent is prohibited except in specific limited circumstances such as covert surveillance operations and for reasons of national security. The Lawful Business Practices Regulations 2000 set out the exceptions to RIPA and provide the basis under which the Authority's monitoring activity can take place. The Employment Practices, Data Protection Code gives further guidance on how monitoring should be carried out. It aims to strike a balance between the rights of individuals (their privacy) and those of the employers (their ability to monitor activities to ensure their business is operating

effectively). The Authority has used the benchmarks and practical guidance in the Code to help develop the policy for the Acceptable Use of ICT Facilities, particularly in relation to the monitoring of e-mail.

5.10 Obscene Publications, Pornography etc

The Authority is committed to the prevention of publication on its networks of any material which it may consider pornographic, extremist, excessively violent or which comes within the provisions of the Obscene Publications Act or the Protection of Children's Act. In no circumstances should users send e-mails containing pornography or other objectionable or potentially criminal material. If users receive an e-mail that they believe may contain pornography or, on opening an e-mail find such material, for example in an attachment, they should immediately close it and report the incident to Computer Audit (either by e-mail to computeraudit or by telephone on 292771).

Any use of the Authority's ICT systems to publish, distribute, or gain access to obscene, discriminatory, pornographic or excessively violent material will lead to disciplinary action being taken.

APPENDIX A

Vicarious Liability (including the Authority's E-mail Disclaimer)

A.1 The term "vicarious liability" means that the Authority may be held responsible for actions by staff or agency workers if they are deemed to be committed 'in the course of employment'.

This applies when:

- the wrongdoer is employed under **a contract of employment** (generally speaking, an employer is not responsible for the activities of an independent contractor); ***and***
- the employee is acting **in the course of their employment.**

A.2 Managers should be aware that the wrongful act of a member of staff or contractors will be deemed to be done in the course of employment if it is:

- an act authorised by management, or
- a wrongful and unauthorised mode of doing some act authorised by management.

A.3 Whether an act is an independent act or one for which an employer will be held vicariously liable is a question of fact that will be determined by the appropriate court with reference to the particular circumstances.

A.4 Anyone using the Internet should note that although certain materials may be considered legal in their place of origin, this does not mean that they are necessarily legal in the UK. So, if those materials are considered to be illegal in the UK, they will be subject to the application of UK law.

E-mail Disclaimer

A.5 The following statement is Wrexham's full bilingual disclaimer relating to e-mails sent out of the Authority to external e-mail addresses:

This e-mail message and any attachments are confidential and intended solely for the use of the individual or organisation to whom it is addressed. If you are not the intended recipient and have received this e-mail in error, any use, dissemination, forwarding, printing, or copying of it is strictly prohibited and you are requested to contact the sender and delete the material from any computer.

Opinions, conclusions and other information in this message that do not relate to the official business of Wrexham County Borough Council shall be understood as neither given nor endorsed by it.

Please be aware that, under the terms of the Freedom of Information Act 2000, Wrexham County Borough Council may be required to make public the content of any emails or correspondence received. The Council reserves the right to monitor both sent and received e-mails.

Whilst we make every effort to keep our network free from viruses, you need to verify that this e-mail and any attachments are virus-free, as we can take no responsibility for any computer virus which might be transferred by way of them.

Take a look - you can pay, report, request, have your say and find information online at www.wrexham.gov.uk. Save paper - think before you print!

Mae'r neges e-bost hon, ac unrhyw ffeil sydd ynghlwm wrthi, yn gyfrinachol ac fe'i bwriedir ar gyfer yr unigolyn neu'r sefydliad y cyfeiriwyd hi ato. Os nad chi yw'r derbynnydd priodol ond eich bod wedi derbyn y neges e-bost hon trwy gamgymeriad, gwaherddir ei defnyddio,ei hanfon ymlaen, ei hargraffu a'i chopio a gofynnir i chi gysylltu a'r sawl a'i hanfonodd a dileu'r deunydd o bob cyfrifiadur os gwelwch yn dda.

Dealler nad yw Cyngor Bwrdeistref Sirol Wrecsam yn rhoi nac yn cymeradwyo barn, casgliadau a gwybodaeth arall sydd yn y neges hon nad yw'n ymwneud a'i fusnes swyddogol.

Mae'n bosibl y bydd gofyn i Gyngor Bwrdeistref Sirol Wrecsam gyhoeddi manylion unrhyw negeseuon e-bost neu ohebiaeth a dderbynia, dan delerau Deddf Rhyddid Gwybodaeth 2000. Ceidw'r Cyngor yr hawl i fonitro negeseuon e-bost a anfonir ac a dderbynnir.

Tra gwnawn bob ymdrech i gadw'n rhwydwaith yn rhydd o feirysau, dylech sicrhau bod y neges e-bost hon ac unrhyw atodiadau'n rhydd o feirysau, gan nad oes modd i ni dderbyn cyfrifoldeb am unrhyw feirws cyfrifiadurol a drosglwyddir ganddynt.

Edrychwch - Fedrwch chi dalu, cofnodi, gofyn, dweud eich barn a darganfod gwybodaeth ar y we ar www.wrecsam.gov.uk. Arbedwch bapur - meddyliwch cyn argraffu!

APPENDIX B

Software

B.1 The software necessary for employees to do their job must be installed on their computers by the ICT Service. Responsibility for arranging this for new employees lies with their manager.

B.2 Some posts in the Authority require the use of specialist software. Users who want to obtain specialist software should contact the ICT Service or their departmental MIS / ICT co-ordinator once they have obtained authorisation from their manager. Consideration should always be given to the need to carry out a Privacy Impact Assessment when purchasing new software. All software must be purchased in line with the Authority's Procurement Policy a copy of which is available on the Intranet - SAM.

B.3 Users should not, in any circumstances, open an e-mail attachment containing a software application without first obtaining approval from the ICT Service, if in doubt, contact the ICT Service. Failure to do so might result in the system or network failing and might, in some circumstances, infringe licence agreements.

B.4 Managers should not allow the use of software applications unless they are satisfied that the ICT Service has approved their use. Failure to check might result in the Authority becoming liable for the unlicensed use of copyrighted software applications. Similarly software upgrades provided by vendors should only be loaded with the prior agreement of the ICT Service.

APPENDIX C(1) Other Wrexham County Borough Council Users (e.g. Councillors, Contractors, non-Council / agency staff working for Wrexham, temporary users, other local Authority staff, staff from other public sector partner organisations and existing Wrexham staff who have not previously signed the Acceptable Use Policy)

Statement of Agreement to use Wrexham County Borough Council's ICT Facilities

Please print this page and then:

i) Complete sections (a) to (e) below in ink:

(a) Name: _____

(b) Organisation: _____

(c) Job Title: _____

(d) Contact Number: _____

Authority Employee Responsible for Supporting the Request to Use the ICT Facilities, if appropriate.

(e) *Name:

Department:

Job Title:

Telephone Number:

ii) Ensure you understand the provisions of the Acceptable Use of ICT Facilities Policy;

iii) Sign and date the form and return it immediately to C&CS Dept, ICT Services, Old Library, Queens Square, Wrexham, LL11 1AT. **NOTE** – ICT Facilities will only be made available after a signed and dated copy of this form has been received.

STATEMENT

I agree:

- to abide by Wrexham County Borough Council's Acceptable Use of ICT Facilities Policy and Guidelines;
- to check the Intranet regularly to find out about policy changes;
- to take all precautions necessary to keep the Authority's network and servers secure;
- to ensure that my e-mail correspondence does not contain information that could damage the Authority's reputation or its relationships with clients, outside bodies, or the general public;
- to comply with the requirements of the Data Protection Act;
- to use the Internet access provided by the Authority for work purposes only (in the case of Members of the Council appropriate usage includes that described in section 1.3);
- that the Authority may monitor, inspect, record and disclose as it deems appropriate, all of my Internet, E-Mail or any other ICT-related activity;
- that policies on acceptable use may be amended to remain relevant in the light of technological, legal or organisational developments and that it is my responsibility to periodically check the Authority's policy and guidelines. I agree that any changes

made to the policy in this way will not normally require my signature to indicate my acceptance.

Signature _____ Date _____

APPENDIX C(2) Business E-mail Accounts

A Business E-mail Account is an e-mail address used as a generic contact point for departments. Such accounts are required when it is not always appropriate to direct correspondence to a specific named individual. However, a named individual must agree to monitor the business account to ensure that all e-mail messages received are dealt with promptly and that e-mails are deleted or archived once they have been dealt with.

Internal examples include: *Committee Room 1 - for booking meetings;*
ICT Servicedesk 2340 - for dealing with ICT-related matters.

External examples include: *counciltax@wrexham.gov.uk for Council Tax issues; or*
webmaster@wrexham.gov.uk for website issues.

Statement agreeing to take responsibility for maintaining a Business E-mail Account

Please print this page and then :

(i) complete sections (a) to (e) below in ink:

(a) Name: _____

(b) Department: _____

(c) Job Title: _____

(d) Contact Number: _____

(e) Business Account Name: _____

(ii) sign and date the form and return it immediately to:

C&CS Dept, ICT Services, Old Library, Queens Square, Wrexham, LL11 1AT.

STATEMENT

I agree:

- to abide by Wrexham County Borough Council's Acceptable Use of ICT Facilities Policy and Guidelines;
- to check the Business E-mail Account regularly to deal with all incoming e-mail;
- to take all precautions necessary to keep the Authority's network and servers secure;
- to ensure that my e-mail correspondence through the Business Account does not contain information that could damage the Authority's reputation or its relationships with clients, outside bodies, or the general public;
- to comply with the requirements of the Data Protection Act;
- that the Authority may monitor, inspect, record and disclose as it deems appropriate, all of my Business Account activity;
- that policies on acceptable use may be amended to remain relevant in the light of technological, legal or organisational developments and that it is my responsibility to periodically check the Authority's Intranet site SAM for changes to the policy and guidelines. I agree that any changes made to the policy in this way will not normally require my signature to indicate my acceptance.

_____ _____

Signature **Date**