Staff Acceptable Use of School ICT Facilities

Policy and Guidance

2012

June 2012

Wrexham County Borough Council believes that the use of information and communication technologies in schools brings great benefits. Recognising the issues and planning accordingly will help to ensure appropriate, effective and safe use of electronic communications.

WCBC Children and Young People Services

	Children and Young People Services			
	Department	Learning and Achievement		
	Authors	Simon Billington / Ian Land / Karen Kilcoyne / Sue Robins		
	Approved by			
	Issue Date / Number	June 2012 / final_v1		
	Title	Staff AUP for ICT – Schools		
	Pages 21		**Reference**	SB_SchoolsAUP

CONTENTS Page

1. INTRODUCTION

1.1 This Acceptable Use Policy applies to employees, and other external adult users of the Schools ICT (Information Communication Technology) facilities provided or supported by the School or Wrexham County Borough Council (WCBC).

1.2 ICT facilities include:

- Desktop and Mobile Computing facilities
- Audio-Visual equipment
- Access to the schools / WCBC network
- Access to systems and data provided for school business use
- Access to the Internet and schools Intranet for business use
- Access to the schools e-mail system; and
- Any other approved ICT facilities.

1.2 Definition of a User

1.2.1 A user is defined as any member of staff, including teachers, teaching assistants, governors, temporary workers, contractors and any other adult user who has been assessed and approved for controlled access, and who is provided with school ICT facilities either on a standalone basis or with controlled access to the schools / WCBC network.

1.3 Document Structure

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

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

    - General use of ICT facilities
    - Use of ICT hardware - PCs, laptops, hand held devices, printers, telephones, scanners etc.
    - Use of software – systems applications, databases, utilities [eg MS Office] etc.
    - Internet use
    - E-mail use
    - 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.)
    - Data Security

2. Users' responsibilities and what "Acceptable Use" of the facilities means.
3. What monitoring will take place to confirm compliance with the policies.
4. What will happen in the event of non-compliance.
5. The main legal issues that the policies need to address.

1.4 **Purpose**

1.4.1 The purpose of this policy is to provide a framework for the acceptable use of ICT facilities within WCBC schools. These rules are in place to protect the user and School. Inappropriate use of ICT facilities exposes the school, WCBC and employees to risks including virus attacks, compromise of network systems & services, data security and legal/employment issues.

1.5 **Scope**

1.5.1 This policy applies to all employees and casual/relief/supply staff and other adults using the School's ICT facilities, including all personnel affiliated with third parties. This policy applies to all services, systems and equipment that is owned or leased by WCBC or the School. The ICT Acceptable Use policy applies whether or not the systems are used outside school hours or outside the school.

1.5.2 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 Schools Intranet and a global email will be sent providing a link to the revised policy. Users should therefore periodically visit the Authority's Schools Intranet site to check for changes to the policy and guidelines.

1.5.3 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.

1.5.4 This policy will be reviewed periodically, and following appropriate consultation will be re-issued; as stated in 1.5.2 above.

1.5.5 If there is anything in the guidelines that is unclear, or if you have any specific questions about the policies or concerns about ICT monitoring, please contact your headteacher or the ICT Helpdesk (01978-292380 or by sending an e-mail to icthelpdesk@wrexham.gov.uk)

1.6 **Associated Documents**

1.6.1 This document should be read in conjunction with the following guidance and polices:

- Local Authority eSafety Guidance document – published September 2009
- The schools own eSafety Policy
- The schools own Child Protection Policy
- The Schools own guidance / policy on Data Protection and Security

2. POLICY STATEMENTS

2.1 General Use of ICT

2.1.1 The schools ICT resources are intended for educational and management purposes, and may only be used for activities consistent with the rules of the school. Any expression of a personal view about the school or WCBC matters in any electronic form of communication, including social networking sites, must be endorsed to that effect. Any use of the network that would bring the name of the School or WCBC into disrepute is not allowed.

2.1.2 The School and WCBC provide these ICT facilities on the basis that users:

- Read, understand and abide by the policy statements contained within this document; and

- Sign the “Staff Code of Conduct for ICT” (See Appendix C) to show their acceptance of the policy statements contained therein.

2.1.3 WCBC and the School will ensure that its ICT facilities are protected including:

- Anti Virus Software
- Anti SPAM and Malware protection
- Web Filtering

2.1.4 Users should do nothing to endanger the security or integrity of the School’s systems. External files, such as those listed below, can introduce malicious software, such as computer viruses or worms, that can damage the School’s systems and networks:

- Received as e-mail attachments
- Downloaded from the internet
- Received on CD/DVD disks or other computer media
- On USB memory sticks; or
- Received via any other data storage device

2.1.5 It is important that users do not open or distribute external files unless they were expecting to receive them from a known source or unless authorised to do so by the WCBC, IS Department. Users should immediately contact their schools Network Manager or telephone the IS Helpdesk on 01978 292380 if they suspect that an external file contains a virus. Suspect files must not be opened, uploaded or distributed until the Network Manager / IS department has completed its investigation.

2.1.6 All ICT activity is monitored for appropriate use - See Section 5.

2.2 Use of Hardware

2.2.1 ICT Hardware (PCs, laptops, PDAs, scanners, digital cameras, printers, telephones, mobile phones etc.) provided by WCBC or the School **must** only be used for work purposes relating to the School’s business or as directed by the Headteacher. *The exceptions to this are the limited personal use of e-mail described in paragraph 2.5.4.*

2.2.2 The use of personally owned ICT equipment, e.g. laptops, mobile phones, PDA’s, MP3 players, USB memory sticks etc., to connect, upload or download data on the schools network is not permitted without the knowledge and consent of the Headteacher. *See notes on Data Security and Storage in section 2.8.*

2.3 Use of Software

2.3.1 ICT Software (MS Office, Educational software, graphic and design packages etc.) provided by the School must only be used for work purposes relating to the School’s business or as directed by the Headteacher.

2.3.2 Users must not make unauthorised copies of copyrighted software or digital content, except as permitted by law or the owner of the copyright.

2.3.3 Installation of software and upgrades provided by vendors for existing applications should only be loaded with the prior agreement of the Network Manager, Schools ICT coordinator or IS Department as appropriate.

2.3.4 Installation of software downloaded from the Internet is not permitted without the prior agreement of the Network Manager, Schools ICT coordinator or IS Department as appropriate.

2.3.5 Loading unauthorised or personally owned software (which has not been approved by the school or IS department) can expose the school network to viruses and cause damage to computer operating systems and the wider network. It is therefore not permitted for users to

load personal or non-business related software or files on to any school or WCBC owned ICT equipment.

2.3.6 Users should be aware that any installation of software must be in accordance with the licensing agreement for that software.

2.3.7 It is prohibited for users to recklessly access or transmit information about, or software designed for, breaching security controls or for creating computer viruses.

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

2.4 Internet Use

2.4.1 The School recognises that access to the Internet is an essential tool and can provide significant educational and professional benefits for teachers and school staff.

2.4.2 Users may use the Internet to view or download information only for the purpose(s) of:

- Researching and downloading content that is relevant to the users work within the school, part of ongoing professional development or relevant to the users role as a member of the school community; or

- Participating in forums, news groups and other information exchanges that are relevant to the users work with the school, part of ongoing professional development or relevant to the users role as a member of the school community; or researching topics as directed by the Headteacher.

- 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 WCBC staff, school employees or any other user provided with access. All users must comply with the terms set out in section 3 of this policy relating to Legal Issues when using Internet facilities.

Social Networking Sites

2.4.3 Members of staff, employees and casual/relief/supply staff will not engage in dialogue about the school or with parents and pupils through the use of social networking sites without the express permission of the Headteacher.

2.4.4 The inappropriate use of social networking sites by staff is governed under Wrexham's Corporate Code of Conduct and the General Teaching Council for Wales' Code of Professional Conduct and Practice for Registered Teachers.

2.4.5 Where Social Networking Sites are being used as part of the school curriculum or as part of the school's business they should only be used with the express permission of the Headteacher and should be set up expressly for that purpose. Advice should be sought from the school's ICT Advisory team (01978 317630 / 317632) on appropriate sites to use and privacy settings.

2.4.6 The uploading to social networking sites, forums or internet web sites of any photograph's of individuals or groups taken on school premises is not permitted without the express permission of the individuals concerned. See section 2.9 on the taking of photographs.

Internet Web Filtering

2.4.7 Access to the Internet from the School'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.

2.4.8 If users are aware that a web site is blocked when access is actually required for valid reasons, then a request can be made to allow access to the site. Where a school has local control to its web-filtering server, as is the case in most secondary schools, this can be done internally following the schools web site unblocking procedures. For primary schools and other facilities that do not have local access to release sites, an initial request should be made to the IS ICT Helpdesk on 01978 292380. Where further clarification is needed the IS ICT Helpdesk will contact the schools own ICT Adviser.

2.4.9 Where access to web sites is required for use with learners then sufficient time should be allowed to check the site can be accessed or released before the lesson.

2.5 Use of E-mail Policy

2.5.1 All members of school staff have access to a school email account provided by WCBC and managed by the IS department. This should be used in all situations where email communication is used as part of either WCBC or school business.

2.5.2 ***a) External E-mail***

- All external e-mail will automatically include the Authority's standard bilingual disclaimer statement, which is included in Appendix A.
- Users should not open any file attached to an external e-mail unless they were expecting to receive it from a known source. If you are not certain of the origin of a file, **DO NOT** open it. Telephone the IS ICT Helpdesk on 01978 292380 and they will check the content.
- 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. Further guidance on how to encrypt emails using WinZip is available on the schools intranet. For any further clarification contact the IS ICT Helpdesk on 01978 292380
- 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 or the school

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

2.5.3 ***b) Internal E-mail***

- E-mail is acceptable as a standard form of internal communication except for correspondence:
    - o that requires the signature of a Headteacher – this should be sent by memo;
    - o marked personal or confidential, which contains sensitive or personal information relating to an individual or identifiable person.

2.5.4 ***c) Personal Use of E-mail***

- Headteachers may allow e-mail facilities to be used to send personal messages provided this does not impinge upon its use for official purposes ***and is confined to outside working hours.***

- To ensure privacy, users should include the word "Personal" in the subject line of any personal messages sent. 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 misconduct / crime is suspected.

- All of Wrexham's e-mail facilities are monitored. If through this monitoring it is discovered that e-mails are being sent which contain defamatory, obscene discriminatory, libellous, 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.

2.6 Use of Mobile and Remote Computing Facilities

2.6.1 WCBC and the school recognises that mobile computing facilities provide a valuable educational benefit to the School. This includes provision of Authority or School supplied laptop, PDA, palmtop, Smartphone and other handheld computers, and could include facilities for remote access to the Council and School network from home or other remote locations, in support of work life balance and other initiatives.

2.6.2 For laptops and other mobile devices it is strongly recommended that encryption software be applied to the device, particularly if it is likely to be used for sensitive and/or personal information. For further advice and guidance relating to encrypting such devices, contact the IS ICT Helpdesk 01978 292380.

2.6.3 Any user provided with mobile computing facilities must:

- Use them responsibly and comply with all relevant policies and procedures as if they were using the systems in the their normal place of work
- Take appropriate measures to ensure the physical protection of equipment from loss, theft, damage etc.
- Ensure that any passwords required for access are kept secure
- Return the equipment to the School or IS department when requested to do so for routine maintenance or other purposes

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

- Store files which contain personal and/or sensitive information on the device for longer than necessary unless adequate password and encryption protection has been put in place.
- Download files from the Internet to Authority supplied equipment unless otherwise agreed with the Headteacher.
- Install software, without the prior approval of the schools Network Manager or Headteacher.
- Leave the equipment unattended, even for a few minutes, particularly when travelling away from the office or attending events.
- Take school's ICT equipment, including laptops, PDA's, cellular telephones etc. abroad without specific approval of the Headteacher

2.7 Use of Personally Owned Computer Devices

2.7.1 With regard to computer devices owned personally by users (e.g. handheld devices, laptops, digital cameras, mobile phones, USB memory sticks, MP3 Players etc.), which are not supplied by the WCBC or the School, Users must not:

- Use their own mobile devices to store (download or upload) any organisational information, photographs, record audio or video of children or other members of staff without the express permission of the Headteacher; or

- Connect such devices to the School network (whether remotely or on-site) for any purpose unless without the express permission of the Headteacher.

2.8 Data Security

2.8.1 In carrying out their functions, Schools are often required to hold certain personal and/or sensitive information relating to staff, pupils, parents and other 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.

2.8.2 WCBC and the School have 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'.

2.8.3 All staff should make themselves aware of the requirements of the Data Protection Act and further guidance is available on the School's Intranet.

2.8.4 As a minimum when staff are away from their desks they should ensure that access to their computer / data is prevented by using the Ctrl-Alt-Delete command to lock their PC.

Data storage

2.8.5 Wherever possible the use of removable media should be avoided for transferring or storing data, and users should not use any personally owned removable media or computing device to download sensitive and/or personal school data on pupils or other staff. This includes exam related data.

2.8.6 Storage devices such as removable hard drives or USB memory sticks that do have to be used to transfer or store personal and/or sensitive data must be encrypted and sourced from Wrexham's IS department.

2.8.7 The USB memory sticks provided by the IS department 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 through the IS department by contacting the IS ICT Helpdesk on 01978 29 2380.

2.8.8 As encryption software cannot be easily applied to DVD's and CD's they should never be used to store personal and/or sensitive information / data. Similarly floppy disks, although an older technology, must never be used to store personal and/or sensitive information.

2.8.9 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 Headteacher. Such devices must not be connected to any school ICT equipment unless otherwise agreed by the Headteacher. They must not be used to store any personal and/or sensitive data.

Secure Data Transfer

2.8.10 There are many valid reasons why schools will need to share information with external bodies and partners in order to deliver services or meet contractual arrangements. The external bodies involved can include other schools, WCBC, other Local Authorities, Welsh Assembly Government, examination bodies, public organisations (such as the Health sector), Police, UK and devolved government agencies; as well as private sector companies or individuals providing services or support.

2.8.11 A Privacy Statement has now replaced the Fair Processing Notice and this sets out for data subjects the main reasons for transferring information between schools, WCBC, other Local Authorities and Welsh Assembly Government etc. This notice is kept under review and can be viewed on the schools intranet site and WCBC internet site.

2.8.12 In all cases the reasons for needing to share information should be properly assessed and fully justified. This assessment must include consideration of the degree of sensitivity of the information involved, whether the data is really needed and, if so, can it be kept to the absolute minimum required for the purpose.

2.8.13 Where regular transfers of information take place systems and guidance will have already been issued and should be used to supplement this document.

2.8.14 Any data which relates to individuals must be dealt with in accordance with the Data Protection Act (DPA) and the Schools Data Protection policy. Before any personal data is transferred appropriate justification must be considered and safeguards followed.

2.8.15 **Transfer Mechanisms**

- Where transfer must occur, this should be through secure electronic transfer, so that disks are phased out where possible.
- Where data has to be put onto removable devices or media, such as external hard drives, CD/DVD disks, USB Sticks or laptops etc., these must be encrypted.
- Wherever possible, data should not be transferred but accessed directly through the primary host system where the information is stored, or accessed remotely via a secure channel.

2.8.16 **By Email**

- Email is not a secure method of transfer and should not be used for sending personal or sensitive data unless other viable transfer options have been properly considered and excluded first.
- Personal or sensitive information should never be included in the body of an email.
- If, having considered alternative options, email is considered to be the only viable option for sending the data, then strong encryption must be applied to the data. Email within the Wrexham schools hosted network is secure but encryption should be used. (All schools have been provided with software to support password protection of files
- If email is used you must carefully check the address of the external recipient(s) before sending and contact them afterwards to confirm receipt.

2.8.17 **By Fax**

- Personal or other sensitive data must not be sent by fax. Sending by Fax is not a secure method of transfer as there are inherent risks.

- It may be possible to send non-sensitive data by fax provided the following safeguards are followed. If sending non-sensitive data by fax transfer you must carefully check the fax number of the external recipient before sending. Information should only be sent to “safe haven” fax machines situated in a secure constantly staffed area and not accessible by the public.

- In all cases, the recipient should be informed prior to transfer and a covering sheet addressed to the recipient should be sent with the data. The covering sheet should not include any details of personal or sensitive data.

2.8.17 **By post** (for example in paper form, or, on a CD-ROM or DVD-ROM)

- Sending by post has some risk but provided that strong encryption is applied to data in electronic form and a secure postal service used, the risk is likely to be acceptable.

- Before sending any information to external bodies you must have the approval of the Headteacher.

- If the data is personal or sensitive then strong encryption must be applied (If required contact the IS ICT Helpdesk on 01978 292380 for advice on appropriate encryption levels before sending sensitive data by post).

- The encrypted data must be sent via tracked/secure mail or courier and not via standard post.

- You must carefully check the address of the external recipient(s) before sending and contact them afterwards to confirm receipt.

2.8.18 **By handover** of data to an individual from another organisation

- This has some risk but could be an acceptable method of transfer if an authorised school employee is visiting or can deliver direct to a named external recipient, or, alternatively, if the named external recipient can collect in person.

- If the data is sensitive then the risk must be considered and the need for strong encryption must be assessed

2.8.19 **Taking data off the premises**

- Users should assess the risks of taking data off the premises to meetings or to work on elsewhere. Particular care should be taken during transportation to prevent loss or theft and items should not be left unattended. Information in paper hard copy form should be secured in a box or briefcase/bag and if transporting by vehicle the data should be placed in the boot and remain out of view.

- Information stored in electronic form (contained in laptops, CD-ROM, DVD-ROM or PDAs) must have adequate encryption applied to the device. Personal and sensitive data in electronic form or paper hard copy should not be left in vehicles overnight or for any extended period of time. When handing personal and sensitive data over to a recipient from an external body, the method of transport must be agreed in advance. The IS department can provide advice on the use of encryption.

Loss of ICT Devices and Data

2.8.20 It is the duty of all users to immediately report any actual or suspected breaches in information security to the Headteacher.

2.8.21 If a school ICT device is lost or stolen then it must be reported immediately to the Headteacher and IS Department (IS ICT Helpdesk 01978 292380), this would include the loss of USB memory sticks.

2.8.22 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 Headteacher and IS Department.

Misuse of ICT Devices and Data

2.8.23 You should raise your concern with your line manager, the headteacher, the chair of governors, or the governor nominated for whistleblowing or [*other named person and contact number*]. The person to be approached depends to an extent on the seriousness and sensitivity of the issue and who is thought to be involved.

2.8.24 If you feel you cannot express your concerns within the school, it is open to you to raise your concern with someone outside the school setting from the list of organisations in the section of this policy 'Taking the Matter Further', with key organisations to contact suggested as the LEA, Public Concern at Work and the trade unions.

~~2.8.23 If staff are concerned that school ICT devices or information and data is being used inappropriately then they must inform their line manager and the Headteacher immediately.~~

~~2.8.24 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 the Headteacher.~~

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

If you remain concerned and/or feel unable to raise the matter as detailed above, please refer to the model Whistleblowing Policy for Schools, produced by the Welsh Government at:

English version
http://wales.gov.uk/pubs/circulars/2007/1949006/schoolsandmodelpolicy.pdf;jsessionid=MqpQQHpdjzp6YpjVBxTYyJvGBkNbRG8x2pD5Yn2fH6Rq6MTQy9X9!1219044931?lang=en

Welsh version
http://wales.gov.uk/pubs/circulars/2007/1949006/WAGC36-07-w.pdf;jsessionid=MqpQQHpdjzp6YpjVBxTYyJvGBkNbRG8x2pD5Yn2fH6Rq6MTQy9X9!1219044931?lang=en

or

in the Council's Whistleblowing Policy on the Intranet at:

http://www.internal.wrexham.gov.uk/intranet/departments/personnel/whistleblowing.htm

2.9 Use of Cameras and Taking Photographs of Individuals or Groups

2.9.1 In a public place we do not have a right to privacy. Anybody can take a photograph of another person in a public place. On private property however if the owner of the property

has expressly said no to photographs and this is made clear, then you cannot take photographs.

2.9.2 Schools are private properties and users are not permitted to take the photograph of an individual or group without their express permission.

3. LEGAL ISSUES

3.1 General

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

3.2 Data Protection

The School holds a wealth of confidential information relating to its staff, customers, clients and suppliers, much of it in electronic format. The unauthorised release of such information, for example via e-mail, on external storage media would be in breach of the Data Protection Act 1998 and could make individual employees and the Authority liable to substantial fines.

3.3 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. As an employee you should familiarise yourself with the Council's policy on Freedom of Information – a copy is available on Wrexnet.

3.4 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/misconduct is suspected. They will however, still be subject to the normal monitoring described in Section 5.

3.5 Harassment, Discrimination, Victimisation and Defamation

If employees transmit obscene or discriminatory materials or harass or victimise other individuals by e-mail or any other ICT facility, 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 race; gender; gender reassignment; age, disability, sexual orientation, religion or belief; marriage or civil partnership, and pregnancy and maternity. The Equality Act 2010 also provides protection for staff from harassment during the course of their employment from third parties (S40 (2a and b). If any staff feels that they have been harassed by a third party including via ICT such as email or the internet as part of their employment this should reported immediately to the Headteacher. Where ICT is used as part of the harassment the Headteacher will inform the IS Department as part of preventative action against the harassment. See below for useful links to Equality legislation and guidance. **:**

http://www.equalities.gov.uk/equality_act_2010.aspx
http://www.equalityhumanrights.com/

3.6 **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 could be considered as discriminatory, harassment or victimisation. This would include discrimination, harassment or victimisation on the basis of gender; gender reassignment; race; age; disability; sexual orientation, religion or belief, marriage and civil partnership and pregnancy and maternity. This is in line with the requirements of Equality Act 2010 and related regulations and guidance and any other UK equality legislation and employment regulations. The authority is also committed to fulfilling its Public Sector duties under the Equality Act 2010 and related regulations and guidance. This policy supports the general public sector duty to:

- eliminate discrimination , harassment, victimisation and any other conduct prohibited by the Act.
- to advance opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- to foster good relations between persons who share a protected characteristic and those who do not.

3.7 **Software Licensing and Copyright**

Only software that is developed by the School, WCBC or licensed or provided by the developer to the School should be used on the School's ICT facilities. Under no circumstances should users copy software from one PC to another without the appropriate licence agreement. The School could be liable to substantial fines if it was discovered using software without the appropriate licence. (Appendix B explains how to obtain software.)

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).

3.8 **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 School and WCBC has a duty to put procedures in place to prevent unauthorised access. If the Authority and School fails to do this it is likely to be in breach of the Data Protection legislation and could be liable to substantial fines.

3.9 **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.

3.10 **Obscene Publications, Pornography etc.**

WCBC and the School are committed to the prevention of publication on its networks of any material which it may consider pornographic, 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 computer audit or by telephone on 292771).

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

4. USERS' RESPONSIBILITIES

4.1 **General**

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

- Understand and abide by all the policy statements contained within the 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 3, (Computer Misuse Act 1990, Data Protection Act 1998 etc.)
- Use the ICT facilities for work purposes only. Where permitted by Headteacher/Governors the exceptions are:
    - *Limited personal use of e-mail; or*
    - *Limited personal use of Internet - if allowed by the school and in each case providing this is done outside working hours.*
- Use the Ctrl, Alt, Delete command to lock their PC when away from their desk for extended periods of time.

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

- Attempt to use the ICT facilities for any unauthorised purpose.
- Misuse or damage any ICT facilities.
- Load / download unauthorised software or files onto any of the School's or Authority's PC's, laptops or any other school owned equipment.
- Allow external organisations to connect their ICT equipment to the School network.
- Divulge their password to anyone else or leave their password visible on a piece of paper or Post-it note, etc, left on or near their monitor.

4.2 Use of ICT Facilities - E-mail

4.2.1 ***In addition to 4.1 above, when using e-mail, users must ensure that they do <u>not</u>:***

- Send sensitive or confidential information by e-mail - unless otherwise in accordance with the processes outlined in section 2.8.10 to 2.8.19. (E-mails are not encrypted and may pass through several different servers before reaching their destination and could be intercepted at any stage)
- 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 disciplinary proceedings. In addition, the Authority's and or School's reputation can be affected, and they can become liable to legal action, where such e-mail travels outside the school with the Authority's domain name (wrexham.sch.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.

4.2.2 Use of ICT Facilities – Internet

In addition to 4.1, when using the internet, users must ensure that they do <u>not</u>:

- Access web sites which are not work related, unless otherwise agreed with the Headteacher
- Use the Internet facilities for personal use, unless otherwise agreed locally with the Headteacher and outside of work hours.
- Download software or files from the Internet without the permission of the Headteacher.
- Upload information or data to the Internet unless otherwise agreed with the Headteacher.

4.3 **Who to Contact**

To make the most of the ICT facilities, users should contact:

- Their Network Manager, MIS / ICT Coordinator or the ICT Advisory team:
  - For all ICT training needs (if you don't know how to do it, then ask!)
  - For requests for non-standard ICT software
  - Support relating to the curriculum use of ICT;
  - To report any suspected misuse of the School's ICT facilities or information and data.
- The school Network Manager / Technician or IS ICT helpdesk 01978 292380 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
- Or any other issued outlined in this policy document.

- The schools e-Safety Coordinator or Child Protection Coordinator 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.

5. MONITORING

5.1 General

5.1.1 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 and School's ICT facilities and reputation and to confirm compliance with the relevant legislation and Wrexham County Borough Council's ICT policies.

5.1.2 All users must give their formal consent to the School / Authority monitoring their ICT activity. School staff do this by accepting this policy document under their terms and conditions of employment. Other adult school ICT users do this by completing and signing the Statement of Agreement in Appendix C.

5.1.3 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.
- The IS Department 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.

5.2 Non-compliance

If the monitoring in 5.1 above identifies:

- ***evidence of misuse of the ICT facilities -*** this may lead to disciplinary action, up to and including dismissal
- ***evidence of possible criminal activity -*** this may be passed on to the police
- **As a user you have a responsibility to report any misuse of the Authority's and School's ICT facilities and data to your Headteacher or to the WCBC ICT Manager.**

APPENDIX A

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

A.1 Basically, the term "vicarious liability" means that the Authority or School 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 School's 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 Where the school has implemented an email disclaimer this should be attached to all outgoing emails.

APPENDIX B Software

B.1 The basic software necessary for employees to do their job should be installed on their computers by the IS Department or School ICT Technician. Responsibility for arranging this for new employees lies with their line manager.

B.2 Some jobs in the School require the use of specialist software. Users who want to obtain specialist software should contact the IS helpdesk or their relevant MIS or ICT co-ordinator. All software must be purchased in line with the School's ICT Procurement Policy and Guidelines.

B.3 Users should not, in any circumstances, open an e-mail attachment containing a software application without first obtaining approval from the IS Department or school's Network Manager. If in doubt, contact the IS ICT Helpdesk (e-mail icthelpdesk@wrexham.gov.uk or telephone 01978 292380). Failure to do so might result in the system or network failing and might, in some circumstances, infringe licence agreements.

APPENDIX C - Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using Information Systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-Safety policy and the ICT Acceptable Use Policy for further information and clarity.

Use of ICT systems:

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, hand held devices, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will not leave laptop computers or any other easily transportable ICT equipment unattended at any time.
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that e-mail should not be considered a private medium of communication and that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will ensure that electronic communications with pupils and parents including email, IM and through social networking sites are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that my private and professional use of social networking sites remains separate.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any software or hardware without permission.
- I will not introduce floppy disks, CDs, memory sticks or any other device into the system without first having checked them for viruses.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will not take the photograph of any individual or group for which I do not have their express permission.

The School may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read the schools acceptable use policy and agree to follow the schools code of conduct.

Full name: …… **Date:** ……

Signed: ……..

Accepted for the School: …… Date: ……