

Internet Acceptable Use Policy

Objective

This Internet AUP shall apply to all MTCBC employees, school staff and members who will be referred to as 'Internet users'. The objective of the Internet AUP is to ensure the effective and appropriate use of the Internet facilities. While Merthyr Tydfil County Borough Council (MTCBC) is committed to the use of the Internet for business purposes, it must ensure that suitable controls are in place to prevent security breaches or other negative consequences. The primary use of the Internet is for business and education purposes, however, private use will be permitted daily between 12 noon and 2pm for corporate staff (i.e. when clocked out for lunch) and during non-teaching time for school staff. Please note that the correct protocols will still apply. All Internet access may be recorded and monitored.

This policy has been developed to manage the way in which the authority complies within the ISO 27001 standard.

Scope

Internet access refers to the use of any resources from the World Wide Web, whether browsed or downloaded.

Policy Statements

MTCBC's Internet facilities shall be used in accordance with:

- MTCBC's specified and published principles and policies;
- All appropriate legislation.

Internet usage may be monitored to ensure compliance with this Internet AUP. Any updates will be passed to the Governing Body for acceptance in regards to schools and full Council regarding corporate use. The Internet AUP is approved by, and has the full support of the Chief Executive.

Implementation responsibilities

The Information Security Officer shall develop, maintain, and publish processes to achieve compliance with this Internet AUP. Any queries regarding this AUP can be directed to 01685 727444 or via email, information.security@merthyr.gov.uk .

All Heads of Service/Head teachers shall be responsible for implementing the Internet AUP within their areas of responsibility.

All Internet users shall sign the Information Security Policy to indicate their agreement to comply with the Internet AUP.

Internet Usage Principles

- a. It is a matter for managers/head teachers to approve who can use the Internet and to determine the level of access required. Corporate users and members must submit a "Request for ICT Services" form to the ICT department. Corporate users requesting Internet or External Email must have the form authorised by your Head of Service. Head teachers should approve the use of the Internet for school staff.
- b. Connection to the Internet will be performed by the ICT department. This is to ensure that maximum control and protection is achieved and to promote for quality in-house technical support on any matters arising. Corporate staff or Councillors must not connect to the Internet on County Borough equipment via other Internet Service Providers under any circumstances. School based staff that have a business requirement for this must refer to, and adhere to the 'School Remote Working Policy'.
- c. Messages or images shall not be posted on any Internet message board or other similar Web based service that would bring MTCBC or the school into disrepute, or which a reasonable person would consider to be offensive or abusive.
- d. Internet users shall not place on the Internet any opinion or statement that might be construed as representing MTCBC or the school.
- e. Internet access shall not be used for financial gain, or to host a website on any MTCBC or school equipment.
- f. MTCBC shall report any illegal activity to the Police. Employees shall also be liable to MTCBC's own disciplinary process, members shall be in breach of MTCBC's Members Code of Conduct and a case will be presented to school governors to consider disciplinary action against school based staff.
- g. Internet users' use of the system shall not have a noticeable effect on the availability of the system for other users. Internet users shall not participate in on-line games or have active any web channels that broadcast frequent updates to their computer (with the exception of games and web channels used in a learning environment for educational purposes).
- h. Internet users should not visit Web sites that display material of pornographic nature, or which contain material that may be considered offensive. Corporate staff and members shall notify the Information Security Officer immediately should accidental access to such material occur. Teachers should inform the head teachers. No disciplinary action shall be taken against employees who accidentally access sites containing dubious or unethical material providing they advise the Information Security Officer/head teacher in a timely manner. However, in order to avoid disciplinary action, it is the Internet users' responsibility to ensure that such unauthorised access does not happen on a frequent basis.

The following is not an exhaustive list but an indication of the types of conduct that may result in disciplinary action and possibly dismissal:

Creation, use, transmission or encouragement of material which:

- Is illegal, obscene or libellous;
- Is offensive, abusive, sexist, racist, defamatory or annoying;
- Infringes another person's/organisation's copyright and/or other statutory, regulatory and/or current law prescriptions;
- Transmission of unsolicited commercial or advertising material;
- Obtaining unauthorised access to MTCBC's/schools or other organisation's ICT facilities;
- Violating other people's privacy;
- Using chat lines or similar services (forums are permitted when used in an educational context);
- Playing games (other than when used in an educational context);
- Illegal activities including breaching the Data Protection, Computer Misuse and Design Copyright and Patents Acts;
- Wasting network and staff resources;
- Disrupting other user's work in any way, including by viruses or data corruption;
- Expressing personal views, which could be misinterpreted as those of MTCBC or the school;
- Committing MTCBC or schools to purchase or acquiring goods or services without proper authorisation;
- Downloading copyrighted or confidential information;
- Using the Internet to an excessive degree. If the line manager or Head teacher considers that the Internet is being used more than is necessary for the business function then the facility may be withdrawn.

i. Misuse: this includes, but is not limited to, excessive time, large downloads, games, chat rooms, discussion groups, movies or film clips (games, discussion groups, movies or video clips are permitted when used in an educational context), advertising personal goods or services, online trading, sending unsolicited email (the practice known as 'spamming') and the introduction of unauthorised software to the system.

j. Inappropriate use: this includes, but is not limited to, pornographic or adult-orientated websites or emails, racist, sexist or gambling websites or emails, sites promoting violence, and illegal software.

k. Where material is obtained from the Internet, ensure that any copyright restrictions are obeyed and that virus protection procedures are followed. Where material MTCBC owns is published, ensure that it carries out copyright indications.

l. Any Internet user using MTCBC facilities to access offensive material will face disciplinary action if they access such data/material deliberately. If illegal material is accessed deliberately, then MTCBC will inform the Police and a criminal prosecution may follow.

m. Corporate staff and members who attempt to access a website that is blocked by the filtering system, but feel that they have a business requirement to access the site, must contact the ICT Helpdesk and log a call. School staff must contact their System Administrators.

n. Internet users shall consider any issues concerning copyright and malicious software, before downloading any files or software from the Internet.

o. Internet users shall not enter their email address on a Website unnecessarily, unless there is a business or education purpose, as this might expose MTCBC or the school to security risks such as malicious software attacks or unwanted junk messages.

p. Internet users logged in at a computer shall be considered to be the person browsing the Internet. Under no circumstances shall Internet users browse the Internet from an account belonging to someone else.

q. The use of social networks (i.e. Twitter, Facebook, LinkedIn, YouTube, Flickr – this is not an exhaustive list) for personal reasons is not permitted during working hours, social networking uses up corporate bandwidth which is there for business use only. Social networking during working hours must be for teaching and learning activity only.

r. When communicating with pupils and parents using social networks, a school identifiable account must be used – all communication will be relevant to the professional role. Social communication with pupils and parents must not involve personal interaction with pupils or parents, or any other third-party, outside of its intended school purpose. Every effort must be taken to ensure messages cannot be perceived as ambiguous or misunderstood.

s. School staff must remember that they are representatives of their school and MTCBC, and using personal or school social network accounts to make libellous, slanderous or defamatory comments regarding their school or MTCBC, or its employees, will not be tolerated and may lead to disciplinary action.

t. Personal information must not be posted on social networks. Personal information is information that relates to a living individual who can either be i. identified from that data or ii. Can be identified from the information combined with any other information that is in the possession of the person or organisation holding the information. Basic personal information includes:

- Name
- Address

- Date of birth
- National Insurance Number

Sensitive personal information includes:

- Racial or ethnic origin
- Physical or mental health conditions
- Offences or alleged offences
- Religious belief
- Sexual life

u. All Internet access is logged and may be monitored.

Policy created by MTCBC