Ysgol Greenfield School

"Opening doors to the future"

CYNGOR BWRDEISTREF SIROL MERTHYR TUDFIL

MERTHYR TYDFIL COUNTY BOROUGH COUNCIL

GREENFIELD SCHOOL

EMAIL AUP POLICY

Wayne Murphy, Head Teacher.
Rachel Faulkner, Deputy Head - Standards
Carol Conway, Deputy Head - Wellbeing
Gwyn Daniels - Assistant Head

' Opening Doors To The Future '

' Agor drysau i'r dyfodol'

Original Completion Date	**Author**
November 2015	Kira John

MONOTORING THE POLICY

This policy will be reviewed bi-annually unless change of circumstances or legislation requires it to be amended earlier.

Signed: …….. Date: ……..

Head teacher

Signed: …….. Date: ……..

Chair of Governors

Review Date **Author**

Our Vision

'To open doors to the future'

Our Mission Statement

That children, staff, parents, carers and all stakeholders work actively in partnership to enable all pupils to realise and reach their full potential.

Aims

- For pupils to operate as independent learners and thinkers
- To inspire a love for learning
- To provide a relevant curriculum for all
- For pupils to value themselves
- To foster a sense of belonging to a community

Our Values

- We create
- We respect each other
- We try our best
- We are a team
- We learn from mistakes
- We celebrate each other's success
- We are polite and considerate
- We produce magic moments

We want every child to be safe and happy in our school. We believe that the key to this is for us all to have self-respect, respect for others and respect for property.

Everyone has the right to:

- Feel safe, cared for and respected.
- Be able to learn to the best of his/her ability and to develop whatever skills he/she possesses.
- Be treated equally irrespective of gender, race, physical characteristics or any other factors.
- Learn and play without disruption.

Everyone is expected to:

- Be responsible for their own behaviour
- Respect the rights of others
- Share our values

Objective

The objective of this policy is to ensure the effective and appropriate use of email.

Scope

The Email AUP shall apply to all email messages processed by MTCBC employees, school staff and members. All employees should remember that standard email is not a secure form of communication. A more secure method of communication shall be used, if the content of an email is sensitive or critical such that if its content were disclosed or modified by an unauthorised person it could cause embarrassment or financial loss.

Greenfield School and MTCBC reserves the right to temporarily or permanently limit, withdraw or restrict use of, or access to, any ICT facilities if they are used in an inappropriate manner.

Email Usage Principles

- Greenfield School provides emails to assist employees and members in the performance of their roles. Whilst its use should be primarily for school business.

No staff shall send or forward emails that in any way may be interpreted as insulting, disruptive or offensive by any other person, company, or which may be harmful to the morale of employees. Examples of prohibited material include, but are not limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files;
- Unwelcome propositions, request for dates, or love letters;
- Profanity, obscenity, slander or libel;
- Ethnic, religious, or racial slurs;
- Political beliefs or commentary;
- Any message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs.

- People receiving offensive or sexually explicit mail should inform the ICT co-ordinator or head teacher immediately and log an information security incident via the E-safety log. Such material may not be identifiable until an e-mail is opened and in these cases, staff will not be held responsible provided they report it immediately.

- Email should be unambiguous and expressed in plain business language so as to minimise the risk of misinterpretation.

- The head teacher will approve who can use the Internet and Electronic Mail and will determine the level of access required. Email users must accept and adhere to the policies fully.

- You should always remember that checks may be made to ensure that misuse is not taking place in the event of suspected or reported misuse. Therefore, you should not expect emails to be private as there is a possibility under these circumstances that the content will be seen by someone other than the sender/recipient.

- The email system shall not be used for personal financial gain.

- Staff shall **NOT** forward chain letters either internally or externally. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. Virus warnings shall come under the same exclusion as the majority of these are false. School staff shall refer to the ICT co-ordinators to check the validity of such messages but shall not forward these messages to anyone under any circumstances.

- Always remember that e-mail messages, however confidential or damaging, may have to be disclosed in court proceedings if relevant to the issues.

- Email addresses shall not be disclosed unnecessarily unless there is a business or education purpose. Information provided in surveys or other questionnaires may lead to risks such as receiving unwanted junk messages.

- School staff shall not subscribe to email lists which are not relevant to business or educational use. The volumes of messages that can be generated are high and the content may be dubious resulting in conflict with the conditions in this policy.

- Care should be taken opening emails and attachments from unknown sources. Caution shall also be exercised even if attachments are received from known sources.

- Users will be made responsible for the security of their username and password and must not allow other users to access their email using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.

- Personal information must not be attached or mentioned in emails. 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

- Users must understand how to use emails. Do not mismanage CC and BCC: only CC in people that really need to receive the email.

- Archive effectively - use folders and delete any messages you no longer need

- Staff Emails are a form of corporate communication and therefore should be drafted with the same care as letters.

- Users should be careful when replying to emails previously sent to a group.

- Ensure your terminal is locked or logged out when you leave your desk, a malicious user could send messages in your name