Blaenbaglan Primary School - Ysgol Gynradd Blaenbaglan
Headteacher: **Mr. D.Burrows**
Deputy Headteacher: **Mrs. E. Palmer**
Maes-Ty-Canol, Baglan, PORT TALBOT. SA12 8YF.
Tel: **01639 769775** Fax: **01639 769776** e-mail: **blaenbaglan@npt.school**

'Together, we believe, achieve & succeed'

Internet Usage Policy
2023/24

Signed:
Date: 05.10.2023
Review Date: Summer '24

Internet Usage Policy

Human Resources

APPROVED BY	Personnel Committee
DATE	
EDITION/VERSION	2
REVIEW DATE	

Signed:
Date:

Contents Page

Appendices

1. INTRODUCTION

1.1 This document updates and replaces the earlier Internet Security - Policy and Advice Note (December 1999). Its purpose is to assist in making legitimate Internet use in the course of County Borough Council business as effective as possible, and to define acceptable and unacceptable uses of the Internet by staff.

1.2 The Internet is a communications and research facility which can be used very effectively to assist in the conduct of the Authority's business. It will also be used to publish information about the Authority's services, and perhaps to deliver some of those services. Like any resource, its use should be limited to legitimate business and is governed by rules of conduct similar to those applicable to use of other resources. While business use of the Internet is to be encouraged, there are serious legal risks, both to the Authority and to the individual member of staff, arising from misuse or the unintended consequences of actions taken.

1.3 The County Borough Council's Internet Usage Policy is set out below.
Appendix 1 contains some general guidance on use of the Internet, including Internet email. Explanations of the legal reasons for the policy which follows are set out in a separate document which is available from accountable and line managers in all directorates.
Appendix 2 sets out new rules for staff access to the Internet with effect from 15th October 2007.

2. COMPLIANCE

To ensure compliance this policy must be given to, and understood by, each user of the Internet service. The Internet Usage Form at the back of this document must be signed by both the user and his/her Head of Service, and filed securely by each Directorate.

3. CONNECTION

Connection to the Internet will be provided only via the Corporate Data Network and Web Server, undertaken at the request of Directorate management. PCs so connected will not be allowed to maintain an additional separate dial-up modem connection to any other processor or network. In addition, any PC which effects a connection to the Internet must have regularly updated virus monitoring software installed.

4. ACCEPTABLE USES

4.1 Uses that are acceptable and encouraged are:

i) Communications and information exchanges directly relating to the aims and business of the Authority.
ii) Use for research, analysis, advisory, professional or development activities related to staff duties.

4.2 Limited personal use is also permitted, provided that:

i) It takes place within staff members' own time, (before 8.30am, between 12 noon and 2.00pm, and after 5.00pm with no exceptions. This will apply seven days per week.
ii) It takes place at no cost to the Authority.
iii) The Authority's email address is NOT used. Staff wishing to send or receive personal emails can open a private account with a free email service. All emails sent and received from NPT email addresses are monitored by the Authority and may be read as part of any service review and /or investigation carried out by Internal Audit or Service Managers.
iv) The New Rules for Staff Access to the Internet set out in Appendix 2 are complied with.

Personal use of the Authority's Internet facilities will be subject to constant review and will be withdrawn if it is misused or if it imposes a cost on the Authority.

4.3 Uses that are unacceptable involve the access, use, submission, publication, display, downloading or transmission of any information which:

i) Violates any of the Authority's regulations.
ii) Violates or infringes on the rights of any other person, including the right to privacy.
iii) Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
iv) Restricts or inhibits other users from using the system or the efficiency of the Authority's computer systems.
v) Results in the unauthorised editing of the Authority's web pages.
vi) Encourages the use of controlled substances or uses the system for purposes with criminal intent.
vii) Uses the system for any other illegal purpose.

4.4 It is also unacceptable to use the facilities and capabilities of the system to:

i) Conduct any unapproved business.
ii) Solicit the performance of any activity that is prohibited by law.
iii) Transmit material, information, or software in violation of any law.
iv) Conduct any unauthorised political activity.

v) Conduct any unapproved fund raising or public relations activities.
vi) Engage in any activity for personal gain.
vii) Make any unauthorised purchases or commitments.

4.5 Warning: All Internet users should bear in mind that a continuous and complete record of all Internet activity, including email, is maintained in respect of all PCs in the County Borough Council. The same legal and disciplinary considerations apply to Internet misuse as to the misuse of other Council facilities. Staff engaging in unauthorised activities may be subject to disciplinary action, up to and including termination of employment and/or legal proceedings.

5. COPYRIGHT

5.1 Users may download copyright material for legitimate business purposes. However, the use of such material must be strictly in compliance with the author's copyright conditions or current copyright law.

5.2 In the case of software, downloads must be authorised by directorate I.T. management and must comply with corporate and directorate information technology policies and standards. Any applicable licence conditions must be complied with.

6. DISCLAIMER

A disclaimer will be automatically inserted into all Council emails sent, to avoid a creation of legal obligation in the event that the email contains a virus or has been intercepted and amended. The disclaimer should be at the top of emails and not the bottom.

7. ENFORCEMENT OF COMPLIANCE

It is the responsibility of Directorate Management to ensure that all Internet users comply with the policies contained within this document. In addition, Internal Audit will, from time to time, undertake monitoring and investigation activities. The DOFCS I.T. Division will also undertake investigations at a Corporate Director's request.

8. INTERNET USAGE CONSENT FORM

All staff having access to the Internet must acknowledge that all network activity is the property of the Authority and that, therefore, no such activity can be considered private. Staff must sign the Internet Usage Form attached in Appendix 3, which must also be countersigned by the appropriate Head of Service.

Appendix 1

SOME GUIDANCE ON INTERNET AND E-MAIL USE

General Internet Usage

A number of guidelines have been published by a group known as Internet Fraud Watch. Most of these relate to business transactions, but a few are pertinent to all transactions which require a user to impart information:

- **Be careful to whom you disclose financial or personal information**. Do not provide bank or credit card details, national insurance numbers or indeed any personal or Authority information unless you know the recipient to be legitimate and that the information requested is necessary for the transaction. Even partial information may be enough for someone to impersonate you on the Internet.

- **Do not judge reliability by how well laid out or professional a web site may appear.** Anyone is able to create, register and promote a web site. It is relatively easy and inexpensive to create a simple site, and as with other forms of advertising, you cannot assume that it is backed up with any form of organisation.

- **Understand what is actually on offer.** Look carefully at the information being presented and ask for more information if required. Any legitimate organisation will be more than happy to accept such a request.

- **Take time to decide.** Beware of anyone offering a short timespan during which their download is available. Such high-pressure tactics are often a sign of fraud.

- **Know that people in cyberspace may not always be what they seem.** The increase in "chat" packages now allows people to undertake real time conversations over the Internet. Remember that anyone could be listening, and that requests for personal or company information should be closely questioned.

- **Unsolicited email violates computer etiquette and is often used for ulterior motives.** It also violates most agreements for Internet service, and is the most common place to find email viruses. An example of this is the email with a text message inviting you to "Open me up to find out how to etc", the virus activating once the email has been opened. The only way to avoid infection is to delete the email prior to opening. This type of email attack is known as "spamming", and while it is not always dangerous, all occurrences should be reported.

- **Do not download programs to see pictures, hear music or obtain other features from websites with which you are not familiar.** To do so could result in the unintended download of a virus. A particularly nasty trick which dial-up users should be aware of, is a download which disconnects your service link and reconnects your PC through an international phone number, resulting in large telephone charges.

Email Etiquette

The proliferation of email services now afforded via the Internet has resulted in large numbers of people conversing electronically. As the electronic community has grown and the number of mail items received appears to increase each day, a number of unwritten rules have formed, the most pertinent of these being reproduced here. These are only guidelines, and will not apply when maintaining a dialogue with colleagues or friends, but they will help to minimise the number of rebukes received from the international community:

- **Be concise.** One of the many benefits of email is its ability to answer a question or communicate a thought in a quick and informal manner. Keeping communications short helps to keep email more productive.

- **Avoid "Flames".** A flame is an inflammatory, critical or junk message. Avoid sending such email, or indeed email which contains insufficient information.

- **Use asterisks.** Asterisks are used to highlight key words or phrases, e.g. "thank you *very* much". Avoid a tendency to overuse.

- **Use "Threads".** Threads are a series of responses to an original message. Instead of starting a new message as a response to mail received, it is often helpful to continue the thread by pressing "reply" to the message and continuing to do so until the communication is complete. Keeping the thread intact will make it easier for any participants to follow the chain of information that has been exchanged.

- **Avoid "Spamming".** Spam, used in this context, is a reference to electronic garbage such as junk email. Sending such mail via newsgroups or to someone you don't actually know is considered "spamming".

- **Avoid large distribution lists.** The prefacing of email with a large distribution list can prove quite daunting to the recipient. To avoid such lists, email your message to yourself and blind courtesy copy (BCC) all the other recipients of your message. The result is that each recipient of the message will only see his or her name at the top of the email message.

- **Don't use ALL CAPS.** This practice is the online equivalent of shouting. It should be avoided unless absolutely necessary.

- **Avoid repeat messages.** Sending the same message more than once to the same person is often perceived as pestering. With over 100 countries utilising email it is often the case that email will take its time to arrive. Be patient before re-transmitting the same message, or sending a follow up reminder.

- **Contact information.** Always provide full and proper international dialling codes and contact information when sending email overseas.

- **Store messages.** Backup email messages to disk for future reference. However, regular housekeeping should be undertaken.

Appendix 2

New Rules for Staff Access to the Internet

10th October 2007

Summary

- Personal use of the Council's Internet Facilities will continue to be permitted provided that all personal use is in an employee's own time and not the Council's time.

- With effect from Monday 15th October 2007, personal use of the Internet will only be permissible before 8.30am, between 12.00noon and 2.00pm, and after 5.00pm – with no exceptions.

- The use of SurfControl software is to be extended, again from 15th October 2007, to provide additional security against abuse of the Council's Internet Usage Policy.

Many staff will have seen and heard the extensive media coverage recently given to internet access by NPT staff in relation to one employee being dismissed, one employee receiving a written warning and two others resigning. A further two employees are being investigated for alleged abuse of the Internet Usage Policy.

There have been some concerns for a little while about employees using the internet for personal use during Council time and discussions commenced a few months ago with the Trade Unions about how these concerns could be addressed. Simultaneously, the introduction of new web and email access software has been piloted.

The Council's Internet Usage Policy clearly states that limited personal use of the internet is permissible provided that it takes place within an employee's own time see 4.2(i), that it takes place at no cost to the Council and that the Council's email address is not used.

The Policy also states that personal use of internet facilities will be subject to constant review, access facilities will be withdrawn if misuse is discovered and that unauthorised activities may be subject to disciplinary action, up to and including termination of employment and/or legal proceedings.

Until last year, all staff access to the internet was recorded, but unfiltered. This allowed access to any website at any time, but, unfortunately, disciplinary action needed to be taken against a number of employees for accessing websites containing inappropriate content and/or images.

The Council subsequently put in place computer software known as SurfControl. This software significantly reduces spam emails and is capable of restricting internet access by website content. This is made possible by means of a website classification system whereby every known website is allocated to one of around fifty categories. For example, expedia.com is categorised as a "travel" website. 888.com is classified as a "gambling" website. Wales.gov.uk falls into the classification of "government".

SurfControl provides the Council with a daily update of the classification of every website in existence.

The introduction of SurfControl means that access by NPT employees to inappropriate sites has already been eliminated, spam emails are greatly reduced and the sending and receipt of improper images has also been stopped.

The next stage in the introduction of SurfControl is to introduce another level of restricted access to the internet in a way which will minimise the risk of staff using the internet for private purposes during the Council's time, but will still enable the Council's internet facilities to be used by NPT staff for personal use.

The Council's E-Government Group has looked at each of the fifty or so SurfControl categories and has sub-divided them into three sections:

- **Access Blocked at all times (Category A)** – websites relating to, for example, adult themes, alcohol & tobacco, downloads, gambling, violence and weapons;
- **No Access Restrictions (Category B)** – examples include computing, education, government, professional organisations, politics, reference sites and search engines.
- **Access Restricted to "Personal Time" only (Category C)** – examples include entertainment, fashion, food & dining, games, job search, kids sites, cars, personal & dating sites, shopping, sports and travel;

Following consultation with trade unions locally, the Council has decided that the following arrangements will apply with effect from Monday 15th October 2007.

Category A websites – access to these websites will be prohibited for all employees at all times. Any attempt to access a blocked website will result in an Access Denied screen being displayed. However, if an employee believes that he/she has a legitimate business reason for being granted access to the website/s in question, advice will be displayed on the screen about what to do next. Arrangements are being put in place at a senior management level which will permit access to such blocked websites to be granted on a selective basis. For example, access to a "gambling" website may be permissible for a Licensing Officer if he/she needs to visit a specific site to carry out his/her duties.

Adult/Sexually Explicit		Peer-to Peer
Alcohol & Tobacco		Phishing & Fraud
Criminal Activity		Proxies & Translators
Downloads		Spam URLS
Gambling		Spyware
Hacking		Tasteless & Offensive
Illegal Drugs		Violence
Intolerance & Hate		Weapons

Category B websites – unrestricted access will be allowed to these websites (subject to any website visits for personal reasons being restricted to before 8.30am, between 12.00noon and 2.00pm, and after 5.00pm.)

Advertisements & Popups		Philanthropic & Professional Orgs.
Business		Politics
Computing & Internet		Reference
Education		Search Engines
Government		Sex Education
Health & Medicine		Streaming Media
Hosting Sites		
Infrastructure		

Category C websites – access to these websites will be prohibited other than before 8.30am, between 12.00noon and 2.00pm, and after 5.00pm. As with Category A websites, it will be permissible on a selective basis for access to be gained to relevant websites within these categories at other times if required as part of an employee's duties with the Council.

Arts		Kids Sites
Blogs & Forums		Motor Vehicles
Chat		News
Entertainment		Personals & Dating
Fashion & Beauty		Photo Searches
Finance & Investment		Real Estate
Food & Dining		Religion
Games		Ringtones/Mobile Phone Downloads
Hobbies & Recreation		Shopping
Intimate Apparel & Swimwear		Society & Culture
Job Search & Career Development		Sports
		Travel
		Web-based E-mail

The use of SurfControl will be monitored over the next few months and any changes needed will be made in consultation with trade unions locally.

Graham Jones, Head of Strategic Personnel
8th October 2007

Appendix 3

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

Internet Usage Consent Form

I, _____ of Blaenbaglan Primary School, Schools Directorate, have read this Policy and agree to comply with all of its terms. I agree that the content of all Internet activity conducted during the performance of my duties will be the property of Neath Port Talbot County Borough Council.

I understand and accept that the County Borough Council reserves the right to monitor and record all Internet activity, with and without notice, and therefore that use of the Authority's Internet facilities is not private.

Signed: _____

Date: _____

Head of Service: _____

Date: _____