Ysgol Cybi

Polisi E-bost Staff Ysgolion / *School Staff E-mail Policy*

(Fersiwn 1, Rhagfyr 2022 / *Version 1, December 2022*)

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu'r hyn y mae'n rhaid i'r ysgol ei wneud er mwyn sicrhau defnydd effeithiol ac effeithlon o e-bost gan staff yr ysgol.

Cefnogir y polisi hwn gan adnoddau ar y dudalen Diogelu Data sydd ar Feicrowefan y Gwasanaeth Dysgu.

About this policy

This policy outlines what the school needs to do to ensure the effective and appropriate use of e-mail by school staff.

This policy is supported by resources on the Data Protection page on the Learning Service Microsite.

Fersiwn / *Version*	**Dyddiad / *Date***	**Crynodeb o newidiadau / *Summary of changes***	**Dyddiad a Dderbyniwyd gan Fwrdd o Lywodraethwyr / *Date Accepted by Board of Governors***
F1/*V1*	Rhagfyr 2022 / *December 2022*	Polisi newydd / *New policy*	30/09/26

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Rhagfyr 2025 / *December 2025*
Yr unigolyn a fydd yn ymgymryd â'r adolygiad fydd: / *The review will be undertaken by:*	Swyddog Diogelu Data Ysgolion / *Schools Data Protection Officer*

5.1. School Governing Body 20
5.2. Headteacher (and/or Person Responsible for Data Protection within the School) 20
5.3. All Staff within the School 21
5.4. Schools Data Protection Officer 21
6. Sending E-mails 21
6.1. Personal and Sensitive Information within E-mails 22
6.2. E-mail Activities and Content 23
6.3. Communicating with Pupils via E-mail 24
7. E-mail Signature 24
8. Classification of Personal Information within E-mails 24
9. Retention and Secure Disposal of E-mails 25
10. E-mail Quotas and Limits 25
11. Suspicious E-mails and Links 26
12. Virus Checking 26
13. Monitoring 27
14. Breach of the Policy 27
15. Review of Policy and Oversight Arrangements 27
APPENDIX A- School Staff E-mail Policy- Headteacher's Checklist 31

1. Policy Statement

This policy outlines what the school needs to do to ensure the effective and appropriate use of e-mail by school staff. This policy will provide guidance on how to manage and thereby reduce the risks associated with e-mail for both the user and the school.

Sharing personal or sensitive information of identifiable individuals via e-mail constitutes processing personal information and therefore needs to comply with the data protection principles under the *UK General Data Protection Regulations (UK GDPR)* and the *Data Protection Act 2018*.

The school's main purpose in providing e-mail facilities is to assist school staff in the performance of their role; to provide teaching and learning activities and to assist in delivering approved business activities of the school.

Only authorised users of the school computer systems are entitled to use e-mail facilities and IT facilities provided by the school for e-mail will not be misused.

Every user of the school's e-mail systems has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard. There is an individual responsibility on all school staff to ensure that they manage their e-mail account correctly.

It is also critical to ensure that the information held within the e-mail systems is managed correctly. If not managed correctly, it is possible to result in inefficient work practices, information overload or loss of information that could result in a data breach.

This policy will help contribute to:

- ensuring that the school is compliant with its requirements under data protection legislation such as the *UK GDPR;* the *Data Protection Act 2018* and the *Freedom of Information Act 2000;*
- ensuring that the e-mail system is not overloaded with unnecessary workload;
- reducing information overload of unnecessary e-mail items which need to be reviewed.

2. Scope

This policy applies to all members of school staff, including temporary workers, other contractors, volunteers, governors and any and third parties with a school e-mail account.

This applies to Hwb (Welsh Government) e-mail accounts and any other official school e-mail accounts.

This policy applies to the use, for the purpose of sending or receiving e-mail messages and attachments, of any IT facilities, including hardware, software and networks, provided by the school.

Risks to both the user and the school will be managed by ensuring the proper use of e-mails by making users aware of what is acceptable and unacceptable. These are based upon both legislative requirements and internal policies and must be followed by all individuals with a school e-mail account.

School staff are expected to maintain the highest standards of professional conduct and practice and are expected to adhere to the key principles of good conduct and professional practice according to the *Education Workforce Council (EWC) Code of Professional Conduct and Practice.*

3. Legislation, Guidance and Policies

The main data protection legislation that this policy complies with is that of the *UK General Data Protection Regulation (UK GDPR)*; *Data Protection Act 2018* and the *Freedom of Information Act 2000.*

This policy should also be read in conjunction with the *Schools Data Protection Policy, Schools Information Security Policy; School Staff Social Media Policy; Schools Data Subject Access Request Policy; Schools Data Breach Policy* and *Schools Retention Schedule.*

This policy is also based on the principles of the '*Code of Professional Conduct and Practice for registrants with the Education Workforce Council (EWC)'* and the *'Education Workforce Council (EWC) Maintaining Professional Boundaries with Learners Guide to Good Practice'.*

4. Definitions

Personal data	Any information relating to an identified or identifiable natural person that can be identified either directly or indirectly from that information. This can be stored electronically, on a computer, or in paper-based filing systems.
Special category data	Information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. Special category data is personal data that needs more protection because it is sensitive.
Processing information	Collecting, obtaining, recording, organising, structuring, storing, retaining, amending, adapting, altering, retrieving, consulting, disseminating, restricting, disclosing, destroying, erasing information or using or doing anything with it.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed information.

E-mail	Messages distributed by electronic means from one computer user to one or more recipients via a network. In addition to textual content, e-mail allows the sender to send photographs, video or sound clips in digital form or files.
Mailbox	The destination to which electronic mail messages are delivered. It is the equivalent of a letter box in the postal system.
Unauthorised	Without a legitimate right.
Cyber security	Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorised access.
Hackers	A hacker is an individual who uses a computer, networking or other skills to overcome a technical problem and who illegally gains access to and sometimes tampers with information in a computer system.
Cyber attack	A cyber-attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organisation.
Risk	Effect of uncertainty on objectives. Risks to individuals: the potential for damage or distress. Risk is often characterised by reference to potential “events” and “consequences”, or a combination of these.
Risk Assessment	The identification and analysis of risks to the organisation’s business objectives.
Impact	What are the consequences of the risk were it to occur. Impact is considered as having either an immediate effect or a future effect.
Likelihood	How likely is it that the risk will occur- uncertainty, chance and probability.
Control	Measure that is modifying risk.
Phishing	Scammers send fake emails to thousands of people asking for sensitive information (such as bank details) or containing links to bad websites. They do this to steal details to sell or perhaps to access information held by organisations.
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
Flaming	A virtual term for venting or sending inflammatory messages in an e-mail.
Spam	Irrelevant or unsolicited messages sent over the internet/e-mail, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.
Computer Virus	A computer virus is a kind of malicious computer program, which when executed, replicates itself and inserts its own code.

	When the replication is done, this code infects the other files and program present on the system.
Spyware	Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.
Trojan horses	A program designed to breach the security of a computer system while ostensibly performing some innocuous function.
Cyber bullying	Any use of social media or communication technology to bully an individual or group.
Encryption	Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data appears scrambled or unreadable to a person or entity accessing without permission.
Authentication	Authentication is the process of determining if someone (or something is who (or what) it claims to be.
Two-factor authentication (2FA)	Two-factor authentication, abbreviated as 2FA, is an authentication process that requires two different authentication factors to establish identity- it means requiring a user to prove their identity in two different ways before granting them access to a system.
Anonymised	To remove identifying information from something (such as computer data) so that the original source cannot be known or identified.

5. Responsibilities

5.1. School Governing Body

The school governing body has the responsibility for:

- monitoring the school's overall compliance and accountability relating to this policy;
- ensuring that the school can evidence compliance with data protection legislation.

5.2. Headteacher (and/or Person Responsible for Data Protection within the School)

The Headteacher and/or the person who is responsible for data protection within the school is responsible for:

- ensuring the implementation of this policy and promoting understanding and compliance with this policy;
- monitoring the implementation and compliance with this policy;
- ensuring personal information within e-mails are kept and processed in line with *UK GDPR*; *Data Protection Act 2018* and the *Freedom of Information Act 2000*;
- ensuring that all staff comply with the *Schools Retention Schedule* and that the school carries out regular housekeeping activities relating to e-mails;

- ensuring that classification levels are used appropriately;
- ensuring staff have appropriate training for using e-mails;
- monitoring that school staff adhere to the principles of the *Code of Professional Conduct and Practice for registrants with the Education Workforce Council (EWC);*
- mandating the use of Multi Factor Authentication in staff HWB accounts in order to protect Office 365 accounts.

5.3. All Staff within the School

All staff employed or volunteering within the school, including teachers, classroom assistants, business support staff and governors are responsible for:

- ensuring understanding and compliance with this policy;
- ensuring the practice of appropriate and proper use of e-mail;
- managing individual school e-mail accounts correctly;
- not using personal or unauthorised e-mail accounts to share personal or sensitive data relating to the school;
- ensuring personal information within e-mails are kept and processed in line with *UK GDPR*; the *Data Protection Act 2018* and the *Freedom of Information Act 2000;*
- adhering to the principles of the *Code of Professional Conduct and Practice for registrants with the Education Workforce Council (EWC);*
- appropriately using classification levels in relation to e-mails;
- fully complying with the *Schools Retention Schedule*;
- keeping within the e-mail account quota;
- being cautious of suspicious e-mails and links;
- undertaking all training offered on using e-mails.

5.4. Schools Data Protection Officer

The Schools Data Protection Officer is responsible for:

- providing advice and guidance to the school regarding information protection and security regarding e-mail use;
- monitoring the implementation and compliance of this policy by the school;
- providing advice and support and leading on the reporting of data breaches relating to personal and sensitive information contained within e-mails.

6. Sending E-mails

School staff should consider whether an e-mail is really required before sending an e-mail.

Standard e-mail is not a secure form of communication. The messages that are sent may be over networks owned by other people. A more secure method of communication will be used, if the content of an e-mail is sensitive or critical such that if the contents were disclosed or modified by an unauthorised person it could

cause embarrassment, distress or financial loss. Care needs to be taken that the potential consequences of sending messages are appreciated.

The individual logged in at a computer will be considered to be the author of any messages sent from that computer account. All school staff will log off or lock their computers when away from their desks; under no circumstances should a user send a message from somebody else's account.

When sending an e-mail, the sender must check that the recipient e-mail address is correct and that no-one else that should not receive the e-mail is copied in as a recipient. It is very easy to send an e-mail to the wrong recipient.

If sending any e-mail where there is a need to conceal individual e-mail addresses, the blind copy facility (bcc) should be used. The blind copy facility should be used when sending to a large number of recipients (particularly external).

Consideration needs to be given before responding to a group e-mail or copying others in the e-mail, if all the recipients need to receive the information. School staff should not send e-mails to all staff unless it is necessary and appropriate for all staff to receive the information.

6.1. Personal and Sensitive Information within E-mails

School staff will not use their personal or an unauthorised e-mail account to send or receive any personal or sensitive data relating to the school or its staff or pupils.

E-mail should not be used to send sensitive personal information without first applying a level of password protection appropriate to the sensitivity of the data.

By default, HWB's e-mail system is configured to encrypt its conversation with other e-mail systems while sending and receiving messages. Please see guide- 'Encrypting e-mail sent from HWB addresses' on the IT Portal for guidance on this- https://desggymorth.ynysmon.gov.uk/support/solutions/articles/50000102041-encrypting-email-sent-from-hwb-addresses-

If sensitive personal information has to be shared via e-mail, the relevant information should be saved in to a Microsoft Word or Excel document. The document should then be password protected and sent as an e-mail attachment. The password should be separately and securely shared with the intended recipient. Otherwise, personal information will need to be de-personalised.

It may be appropriate to use initials instead of full names within e-mails or use a unique identifier where only school staff are able to recognise the individual.

It may be appropriate to ask the recipient to confirm that they have received the e-mail if it contains personal information.

If e-mails containing personal or sensitive information is shared with an unintended recipient or is lost or accessed by an unauthorised user, there may be a data breach that will need to be reported immediately to the Schools Data Protection Officer. The school will comply with the *Schools Data Breach Policy.*

6.2. E-mail Activities and Content

The following are examples of activities and usage that is prohibited by school staff on official school e-mail accounts:

- activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users;
- activities that corrupt or destroy other users' data or disrupt the work of other users;
- unreasonable or excessive personal use;
- activities that violate the privacy of others or unfairly criticise or misrepresent others; this includes copying distribution to other individuals;
- enabling the unauthorised provision of access to school services and facilities by third parties.

No school staff will send or forward e-mails that in any way may be interpreted as insulting, disruptive or offensive by any other person, or company. Examples of prohibited material include but are not limited to:

- illegal material;
- confidential material concerning the activities of the school to a third party;
- sexually explicit messages, images, cartoons, jokes or movie files;
- indecent images, data or other material;
- profanity, obscenity, slander or libel;
- any message which could be viewed as demonstrating hate crime on the basis of race, religion, disability, sexual orientation, transgender identity;
- political beliefs or commentary;
- any message which could be viewed as abusive, threatening, offensive or as harassment, bullying, discrimination or disparagement of others based on their gender, race, ethnicity, sexual orientation, age, marital status, national origin, disability or religious or political beliefs;
- defamatory material or material that includes claims of a deceptive nature;
- anonymous messages or deliberately forging messages or e-mail header information (i.e. without clear identification of the sender) or for 'flaming';
- material which is designed or likely to cause annoyance, inconvenience or anxiety;
- unwelcome propositions;
- unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind.

6.3. Communicating with Pupils via E-mail

School staff will only use an authorised e-mail account to communicate in respect of school business.

School staff will not use their personal e-mail account to communicate with pupils or their family/carers.

7. E-mail Signature

It is good practice to set-up a bilingual signature on e-mail accounts. The signature will appear at the end of e-mail messages. This should contain the school staff's name and contact details. These details should be kept up-to-date.

Setting up a bilingual signature ensures the school presents a professional image and informs the recipient of who the sender is and ways to get in touch.

8. Classification of Personal Information within E-mails

E-mails containing personal and special categories data must be identified using data classification terms (OFFICIAL or OFFICAL-SENSITIVE) within the subject field of the e-mail.

The information classification category is determined on the **harm** that could result from loss or unauthorised disclosure of the information. Information classification category determines how information must be protected/handled.

Classification Category	Impact if the information is lost or disclosed to unauthorised people	Examples of Information
OFFICIAL	Almost all the information the school comes into contact with during the course of the working day will be OFFICIAL information. However, OFFICIAL information also includes personal data that is already in the public domain that if disclosed without consent or loss, would not cause harm or distress to any individual.	Routine reports, published annual reports, out-turn data for key performance indicators, information that is freely available e.g. information on the school website; employees' names and job titles and information that is not commercially sensitive.
OFFICIAL-SENSITIVE	• Cause harm or distress to individuals; • Breach statutory restrictions on the disclosure of information; • Would lead to a breach of confidence to third parties (where information is not in the public domain); • Cause substantial harm or distress to individuals or groups; • Prejudice the investigation or facilitate the commission of crime.	Pupil or staff information for which the school has a duty of care e.g. names, addresses, pupil record.

Personal information should not be included in the subject field of the e-mail.

9. Retention and Secure Disposal of E-mails

School e-mail accounts will also be subject to the data protection regulations and the *Schools Retention Schedule* must be followed regarding e-mails.

School staff will not use their official school e-mail account to store information and as a filing or case management system. E-mail systems should be thought of as a way of delivering and receiving messages- they are not intended for the long term storage and retrieval of messages and attachment files.

E-mails will be deleted or filed as appropriate. E-mails that need to be deleted will be deleted and e-mails that need to be kept in line with the *Schools Retention Schedule* will need to be transferred to an appropriate network folder. The *Schools Retention Schedule* should be applied within the relevant filing system in order to comply with *UK GDPR.* School staff should clean up their e-mail mailbox on a regular basis.

Personal information within e-mails may be provided to individuals as part of Data Subject Access Requests. The school will follow the *Schools Data Subject Access Request Policy.*

Where there is any uncertainty, the school should consult with the Schools Data Protection Officer for guidance on how long to retain e-mails.

E-mails that are no longer required according to the *Schools Retention Schedule* will be deleted permanently from the school's information systems.

Any hard copies of personal information contained within an e-mail will be destroyed in a secure manner.

The *Schools Retention Schedule* can be found on the Data Protection page on the Learning Service Microsite.

10. E-mail Quotas and Limits

All accounts have quota limits placed on them.

Users will receive e-mail notification when approaching their quota limit and are encouraged to follow guidance in this e-mail to manage their account. Once over quota no further e-mails can be delivered to an individual's inbox until they have reduced their storage below their limit.

E-mail that fails to be delivered because a user is over quota is held in the local mail queues for four days and the system will retry periodically to deliver. After four days the e-mail is returned to sender.

E-mail folders will be reviewed regularly by the user and any non-essential messages will be deleted or saved within folders. There are several ways to reduce the mailbox size:

- finding and deleting/transferring large e-mails to an appropriate network folder;
- finding and deleting/transferring old e-mails to an appropriate network folder;
- cleaning up duplicate e-mails from ongoing conversations.

E-mails containing large or multiple attachments should not be sent unnecessarily.

11. Suspicious E-mails and Links

School staff should be wary of unexpected e-mails, attachments and links. E-mails, attachments and links will not be opened unless they are from a known source. Malicious files or links sent via e-mail have the potential to capture passwords, steal school data and render workstations or even the school's network unusable.

Should users receive e-mails which appear suspicious (for example, e-mails with suspect subjects lines) they are advised not to open the e-mail or any included attachments. Instead the e-mail should be deleted and the 'deleted items' emptied.

Caution will be exercised before attachments and links received within e-mails are opened. This will be the case even if the e-mail is from a known source.

The Isle of Anglesey County Council's ICT Service Desk should be notified of any suspicious e-mails so that any pattern of a wider problem or attack can be identified at the earliest opportunity and preventative action taken.

12. Virus Checking

Computer viruses, trojan horses and worms are collectively known as malware. One common method of distributing malware is via e-mail. All e-mail communication through the e-mail gateway is checked for malware.

Checking strategies include: refusing messages containing executable attachments, scanning messages for known malware or a combination of both techniques.

All e-mail received by the school will be passed through a filter before reaching users mailboxes; if the e-mail is identified as Spam, it will be quarantined by the system. School staff should not change the setting of security features on their devices.

Multi Factor Authentication should be activated within staff HWB accounts in order to protect Office 365 accounts.

13. Monitoring

The school/Isle of Anglesey County Council owns the e-mail system which means that all e-mail traffic, both sent and received, including attachments, will be monitored and reviewed and any action deemed appropriate will be taken.

This means that nothing should be taken to be private, even if marked as "private" and/or "confidential" or with any similar wording.

This monitoring will make sure that this policy is effective and that users of the e-mail system are abiding by its content. The monitoring is also to ensure that the school's e-mail systems are working properly.

14. Breach of the Policy

Non-compliance with this policy by members of school staff could lead to serious consequences- this could trigger a disciplinary process under the school's adopted disciplinary policy.

This can lead to putting both the individuals whose personal information is being processed and the school at risk.

If a non-employee breaches this policy (i.e. temporary workers, other contractors, volunteers, governors and any and third parties with a school e-mail account), they may have their contract or arrangement terminated with immediate effect.

15. Review of Policy and Oversight Arrangements

This policy will be reviewed by the Schools Data Protection Officer every three years, unless changes to legislation, codes of practice, policy or guidance requires the policy to be updated sooner.

This policy will be approved by the Learning Service Senior Management Team with the input of the Schools Data Protection Operational Group and will be adopted by the school governing body. Compliance with this policy and related procedures will be monitored by the School Leadership Team and the governing body.

If there are any queries or concerns about anything contained in this policy, the Schools Data Protection Officer should be contacted without hesitation:

E-mail: dpoysgolionmon@ynysmon.llyw.cymru

Telephone: 01248 751833

Address:
Learning Service
Isle of Anglesey County Council
Council Offices
Llangefni
Anglesey
LL77 7TW

Further information regarding data protection can be obtained from the ICO website: https://ico.org.uk/

APPENDIX A

School Staff E-mail Policy

Headteacher's Checklist

No	Actions to be Taken	Has the school got this in place (Yes/No)/ Comments/Dates etc.)
1	The current version of the *School Staff E-mail Policy* has been formally adopted by the School Governing Body.	
2	There is a process in place to continually monitor the school's compliance with this policy.	
3	Personal information within e-mails are kept and processed in line with *UK GDPR*; *Data Protection Act 2018* and the *Freedom of Information Act 2000.*	
4	All staff comply with the *Schools Retention Schedule* and the school carries out regular housekeeping activities relating to e-mails.	
5	Classification levels are used appropriately- OFFICIAL and OFFICIAL-SENSITIVE.	
6	Staff have received appropriate training for using e-mails.	
7	Staff do not use personal or unauthorised e-mail accounts to share personal or sensitive data relating to the school.	
8	Staff are aware to be cautious of suspicious e-mails and links and are always cautious and will report these to the Isle of Anglesey County Council's ICT Service Desk.	
9	Staff use the blind copy facility (bcc) when sending e-mails where there is a need to conceal individual e-mail addresses.	
10	Staff use the encryption function on their HWB account or password protect documents within e-mails if sending sensitive personal information.	
11	Staff use initials instead of full names within e-mails or use a unique identifier where only school staff are able to recognise the individual.	

12	School staff always inform the Headteacher if e-mails containing personal or sensitive information is shared with an unintended recipient or is lost or accessed by an unauthorised user.	
13	Staff regularly review their e-mail folders and any non-essential messages are either deleted or saved within folders.	
14	The school follows the *Schools Data Subject Access Request Policy* and e-mails form part of the search for personal information as part of Data Subject Access Requests.	
15	Staff have a bilingual signature on their e-mail accounts.	
16	Staff do not unreasonably or excessively use their school e-mail account for personal use.	
17	Multi Factor Authentication has been enabled in HWB on all staff accounts.	