Ysgol Cybi

Polisi Diogelwch Gwybodaeth Ysgolion / *Schools Information Security Policy*

(Fersiwn 2, Hydref 2021 / *Version 2, October 2021*)

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu'r hyn y mae angen i'r ysgol ei wneud i sicrhau bod gwybodaeth bersonol yn cael ei rheoli a'i diogelu'n briodol a'i bod yn sicrhau cydymffurfiaeth â deddfwriaeth diogelu data mewn perthynas â diogelwch gwybodaeth.

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

About this policy

This policy outlines what the school needs to do to ensure that personal information is properly managed and protected and that it ensures compliance with data protection legislation in relation to information security.

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*	Ionawr 2021 / *January* 2021	Polisi newydd / *New policy.*	
F2/*V2*	Hydref 2021 / *October 2021*	Newid cyfeiriadau at GDPR i UK GDPR ac ychwanegiadau TG / *Change reference to GDPR to UK GDPR and*	

		additional IT information	

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Hydref 2023 / *October* 2023
Yr unigolyn a fydd yn ymgymryd â'r adolygiad fydd: / *The review will be undertaken by:*	Swyddog Diogelu Data Ysgolion / *Schools Data Protection Officer*

Manylion Cyswllt:

Swyddog Diogelu Data Ysgolion

E-bost:
dpoysgolionmon@ynysmon.gov.uk

Rhif ffôn: 01248 751833

Cyfeiriad:
Gwasanaeth Dysgu
Cyngor Sir Ynys Môn
Swyddfeydd y Cyngor
Llangefni
Ynys Môn
LL77 7TW

Contact Details:

Schools Data Protection Officer

E-mail:
dpoysgolionmon@ynysmon.gov.uk

Telephone: 01248 751833

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

Rydym yn hapus i ddarparu'r polisi hwn ar ffurfiau eraill ar gais. Defnyddiwch y manylion cyswllt uchod. / *We are happy to provide this policy in alternative formats on request. Please use the above contact details.*

Dogfen:
Document:

Templed polisi ar y ddeddfwriaeth diogelu data sef y *Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR*) a *Deddf Diogelu Data 2018* mewn perthynas â diogelwch gwybodaeth. */ Policy template on the data protection legislation namely the* UK General Data Protection Regulation (UK GDPR) *and the* Data Protection Act 2018 *in relation to information security*.

Cyfrifoldeb:
Responsibility:

Cyfrifoldeb corff llywodraethu'r ysgol yw sicrhau bod gweithdrefnau ar waith i sicrhau bod yr ysgol yn cadw gwybodaeth yn ddiogel. Cyfrifoldeb y Pennaeth yw sicrhau bod holl staff yr ysgol yn gweithredu ac yn cydymffurfio. */ It is the responsibility of the school governing body to ensure procedures are in place to ensure that the school keeps information secure. It is the responsibility of the Headteacher to ensure implementation and compliance by all school staff.*

Content **Page**

1. Policy Statement

Data protection legislation aims to protect personal privacy and the rights of individuals about whom data is obtained, stored, processed or supplied. The *UK General Data Protection Regulation (UK GDPR)* requires that organisations have **appropriate technical security measures** to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

In order to operate efficiently, the school has to collect and use personal information about individuals with whom it works with. In addition, it may be required by law to collect, use and share information in order to comply with the requirements of the Welsh Government.

This policy aims to protect the confidentiality, integrity and availability of personal information. The school is fully committed to comply with its data protection obligations and ensuring that personal information is processed securely and is properly managed and protected to ensure that no harm or distress is caused to individuals.

The school will ensure:

- all regulatory and legislative requirements are fully met;
- personal information will be protected against unauthorised access and protected against potential breaches of confidentiality;
- all information assets, IT facilities, systems and devices have appropriate security measures in place and are protected against damage, loss or misuse;
- the on-going confidentiality, integrity, availability and resilience of processing systems and services;
- appropriate security measures, standards and controls are in place to prevent personal data from being accidentally altered or disclosed;
- a secure and trusted environment for the management and storage of information is in place;
- the business requirements for the availability of information and information systems will be met;
- risks are identified and appropriate controls are implemented and documented;
- potential breaches of information are reported and investigated;
- that a process is in place for regularly testing, assessing, monitoring, auditing and evaluating the effectiveness of technical and organisational measures and practices for ensuring the security of the processing and protecting personal information;
- where possible, personal information should be pseudonymised or encrypted and also anonymised if appropriate;
- there is clarity over the personal responsibilities around information security expected of school staff;
- information security education and training will be available to all staff;
- access/requests by third parties are carefully considered before allowing access to data.

2. Scope

This policy applies to all members of staff, including temporary workers, contractors, volunteers, agency workers, school governors and any third parties authorised to access the school's information, information systems or ICT equipment.

This policy applies to all personal information created or held by the school in whatever format (including, but not limited to, paper, electronic, e-mail, film, video, CCTV, photographic images) and however it is stored (for example ICT system/database/network, shared drive, filing structure, e-mail, filing cabinets, shelves and drawers).

This also includes physical and organisational security measures and also covers cybersecurity (the protection of networks and information systems from attack).

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)* and the *Data Protection Act 2018.*

This policy is also based on relevant codes of practice and on guidance published by the Information Commissioner's Office (ICO).

This policy should also be read in conjunction with the *Schools Data Protection Policy; Schools Retention Schedule*; *School Staff E-mail Policy, Schools Data Breach Policy; Schools Data Subject Access Request Policy; Procedure for Sharing Information with Police Authorities in the United Kingdom (Gwynedd & Anglesey); Schools Data Processing Policy and Transferring School Records to the Anglesey Archives Policy*. These are all available on the Data Protection page on the Learning Service Microsite.

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.
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.
Information Commissioner's Office (ICO)	The ICO is the UK's independent body (supervisory authority) set up to uphold information rights. The ICO's role is to uphold information rights in the public interest. This includes dealing with complaints regarding problems accessing personal information from an organisation, or if there are concerns about

	how an organisation has handled information- if the information is wrong, has been lost or disclosed to someone else. Data breaches that are a high risk to individuals are reported to the ICO.
Data controller	The people, or organisations, which determine the purposes for which, and the manner in which, any personal data is processed. The data controller has a responsibility to establish practices and policies in line with legislation. The school is the data controller.
Data users	Includes employees whose work involves using personal data. Data users have a duty to protect the information they handle by following data protection and security policies at all times. Staff employed within schools are data users.
Data processors	Includes any person who processes personal data on behalf of a data controller (other than the employee of the data controller). Data processors could include suppliers which handle personal data on behalf of the school.
Data subject	The individual to whom the personal information relates.
Data Protection Officer	A DPO assists to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
Third-party information	A third party is somebody who is not the data controller, the data processor or the data subject.
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.
Pseudonymised	The process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual.
Anonymised	To remove identifying information from something (such as computer data) so that the original source cannot be known or identified.
Information Systems	Information processing computers or data communication systems.
Integrity	The preservation of the complete, accurate and validated state of information.
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.
Unauthorised	Without a legitimate right.
Cloud storage	Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the internet, or "cloud." It is maintained, operated and managed by a cloud

	storage service provider on storage servers that are built on virtualisation techniques.
App	The word "app" is an abbreviation for "application." It is a piece of software that can run through a web browser or offline on a computer, and on a smartphone phone, tablet or other electronic devices.

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;
- monitoring the performance of the school security measures during special interest visits; via the Headteacher reports to governors and observing whilst visiting the school;
- 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 and all policies relating to data protection and security;
- monitoring the implementation of the policy and security arrangements;
- ensuring personal information within the school is kept and processed in line with *UK GDPR* and the *Data Protection Act 2018*;
- ensuring there is a process in place to protect all personal and special category information within the school;
- managing and monitoring information risks and assets within the school;
- ensuring there is a robust process in place to detect and identify data breaches; to investigate and assess breaches including risks and to share any data breach incidents with the Schools Data Protection Officer;
- ensuring that all staff comply with the *Schools Retention Schedule* and that the school carries out regular housekeeping activities;
- determining the level of access to be granted to specific individuals;
- ensuring that classification levels are used appropriately;
- undertaking regular information security audits and sharing findings with the school governing body and with school staff;
- ensuring staff have appropriate training for the systems they are using.

5.3. All Staff within the School

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

- ensuring understanding and compliance with this policy and all policies relating to data protection and security;

- ensuring personal information is kept and processed in line with the *UK GDPR* and the *Data Protection Act 2018;*
- handling information appropriately and in accordance with the classification levels;
- immediately reporting all actual, suspected, threatened or potential data breaches to the Headteacher and/or the person who is responsible for data protection within the school;
- reporting any lost or stolen devices to the Headteacher immediately;
- understanding what information they are using, how it should be protectively handled, stored and transferred;
- understanding what procedures, standards and protocols exist for sharing information with others;
- fully complying with the *Schools Retention Schedule*;
- undertaking all training offered on systems and devices.

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;
- monitoring the implementation and compliance of the policy and monitoring security arrangements within the school;
- supporting the school with addressing any issues or concerns arising from information security audits;
- supporting the school to ensure that appropriate agreements and contracts are in place with data processors to ensure appropriate information security procedures are in place;
- providing advice and support and leading on the reporting of data breaches.

6. Classification of Personal Information

The school will use appropriate information classifications controls for personal and sensitive information based upon the data classification terms (OFFICIAL or OFFICAL-SENSITIVE).

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.

Document authors and senders are responsible for assigning a classification category to the documents they create and share and protectively marking the document.

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	Routine reports, published annual reports, out-turn data for key performance indicators, information that is freely available e.g.

	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.	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.

When it is decided which classification category applies to information, this needs to be communicated by displaying the classification category on the document or file. This needs to be placed in a prominent place, for example:

- documents- the heading of each page;
- files and folders- on the spine or front of the folder;
- e-mails- in the subject heading;
- databases- where possible, protectively mark information produced or created from databases or using reporting software.

7. Record Status

The school will use the following status to mark records according to importance:

Vital	Records essential to the continuing operation of the school and those records which protect the rights and interests of the school, employees, pupils and the public e.g. contracts.
Important	Records necessary for the continuing operation of the school and which may contain information to support vital records or may be of a historical value e.g. policy.
Useful	Records which may be vital or important to members of staff but are of little value to the school. May be of historical value e.g. correspondence.
Non-essential	Transitory correspondence, purely informational with a very short time value. Includes internal announcements, notice of employee activities, routine business activities and invitations to work-related events.

8. Access Security

All data stored on the school's IT systems and paper records shall be available only to individual members of staff with a legitimate need for access. All users of school

information systems must have the authority to access personal information and only for the authorised purposes.

Authorised individuals will only allow other school staff to access personal information if they also have the appropriate authorisation. The school will ensure that all personal information shall be protected against unauthorised access.

Access to systems and data must have appropriate levels of information security. School user accounts will only allow access to areas appropriate to the account holder's job and responsibilities.

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy. To reduce the risk of unauthorised use or theft, equipment should not be left unattended if at all possible. If it is absolutely necessary to leave equipment unattended, it should be powered down or locked to prevent access.

Computers, screens, mobile devices and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected by being set to lock or sleep that will activate after a period of inactivity. A password or passcode will be required to unlock or wake. Staff may not change this time period or disable the lock. Staff will also physically lock computers, screens and electronic devices if leaving their desks or workspaces for a period of time.

When laying out a workspace, staff should always consider whether information that is being viewed or created could be observed by unauthorised persons, e.g. through a window. It should be ensured that computer screens cannot be viewed by any unauthorised personnel (e.g. a computer screen within a reception area).

All external doors to the school building will be locked at ALL times, as regulated access to buildings is the first line of security. Where a workspace has a lockable door, this must be locked when not in use, or unattended for a length of time, unless this is an emergency exit.

Papers, removable media or IT equipment should not be stored near ground floor windows. Where this is unavoidable, windows should be locked when the workspace is unoccupied and blinds closed. School staff need to maintain a clear desk whenever possible.

Appropriate secure spaces should be available within the school to hold private conversations between staff, pupils, parents/those with parental responsibility and visitors e.g. reception areas that are suitable to share personal information with only those who need to be involved in the conversation without the risk of others overhearing.

Other people's personal information should not be discussed and shared in public areas where conversations can be overheard by individuals who should not receive the personal information.

All visitors to the school must sign in and wear a visitor identification badge whilst on the school premises. This includes parents, helpers, contractors, local authority staff and any

other person that is not school staff. Visitors should be challenged by school staff if they are not identifiable or are left unaccompanied in areas where personal information can be seen or accessed. Visitors should not have unsupervised access to personal information at any time.

9. Passwords and Login Details

All electronic devices and IT systems that contain personal information need to be password protected with access only provided to authorised persons. Authorised users will have a unique user ID (login details) and password or passcode. Different passwords should be used for separate systems and devices.

Passwords and login details should not be written down and should not be shared with anyone else.

It is a requirement that workstation, network and service level systems enforce a password policy of changing every 365 days and meeting a complexity of:

- at least eight characters in length;
- a mix of upper-and lower-case characters;
- a mix of numbers and letters

The above is considered a minimum and it would be best practice to use a longer, passphrase made up of several unrelated words, for example:- Dogs-Litigation-Picnic-230721!

Where it is not possible to enforce password complexity within a system, it is the responsibility of the system administrator to instruct staff that passwords must be manually set to meet these requirements. This requirement applies to all systems, regardless of the fact that the workstation is already protected by a password. It is responsibility of the system administrator to ensure all users of the system have their own username and sharing of credentials is not permitted. This applies to all systems either currently deployed or newly procured.

Information Asset Administrators are responsible for checking system records for anomalous / fraudulent activity. How regularly this should be carried out should be determined by the Information Asset Owner's own risk assessments. Further guidance on the responsibilities of Information Asset Administrators and Information Asset Owners can be found on the Information Governance pages of MonITor or by contacting the Schools Data Protection Officer.

The IT Infrastructure team will disable end user devices which have not been used for a period of 8 weeks.

To allow for auditing of activities, all staff will login with their own login account and not Administrator or root accounts. Separate accounts will be used by IT staff for day to day business activities and those activities which require administrative privileges.

To prevent unauthorised persons from gaining access to workstations, the school will disable the ability to boot computers from unauthorised media such as USB drives.

Where shared access is required to the same workstation, access will always be made via individual user's own logins and not via the unauthorised sharing of passwords.

10. Portable and Removable Devices

The following are examples of, but are not restricted to, portable and removable devices

- laptops, tablet devices, iPods, iPads, mobile phones, MP3 Players, digital cameras etc.;
- DVDs, CDs, USB memory sticks (pen drives or flash drives), external hard drives etc.;
- memory cards, backup cassettes and other devices that have the capacity to hold electronic information.

Portable and removable devices present a high risk of theft, accidental loss, unauthorised access and damage.

Removable media presents a significant risk to the school's data protection compliance and cyber security due to the possibility of data loss or the introduction of malicious code. It is for this reason that the use of removable media is prohibited except for in exceptional circumstances.

Where there is an exceptional business case this must be documented by a Data Protection Impact Assessment (DPIA) which details all relevant risks, the mitigations to be put in place and relevant Data Asset Owner's acceptance of the risks. The DPIA should also document why alternative work methods will not be sufficient to meet the need.

Requests for access to removable media must be made via a ticket on the IT Portal the IT Service Desk and will include a relevant DPIA before access will be granted.

Should the business case for access to, and use of, removable media devices be approved, the following sections apply and must be adhered to at all times:

- all removable media devices and any associated equipment and software must only be purchased by the IT Division and installed by the IT Division;
- non-school/authority owned removable media devices must never be used to store any information used to conduct school business, and must not be used with any school owned IT equipment. These devices will be blocked on school/authority PC's and laptops;
- no removable media from outside the authority is to be used;
- removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.

Where unavoidable, data stored on removable media devices must be encrypted. Removable media purchased by the IT Division will enforce encryption to the AES 256bit standard as a minimum.

It is the responsibility of end users to remember the password for their Council issued removable memory device – should this be forgotten the IT Division will be unable to assist with recovering the data held.

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the IT Service Desk should removable media sustain damage.

Removable media which is no longer required, or has become damaged, must be disposed of securely to avoid data leakage. Removable media should not be simply discarded in general office waste bins - users with removable media which is no longer required should contact the IT Service Desk via the IT Portal and make an appointment to hand them over. The IT Division will then ensure their secure disposal.

Any previous contents of any reusable media that are to be reused, either within the Council or for personal use, must be erased by IT. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools and as such, all removable media devices that are no longer required, or have become damaged, must be returned to the IT Division for secure disposal.

Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

11. Use of Personal Devices

Staff members will not use personal devices or drives (such as USB memory sticks and mobile phones) or non-school owned portable or removable devices to store or share **personal information** relating to school and work business.

School data containing personal information should never be copied to a personally owned device.

12. Protection from Malicious Software and Unwanted Programs

The school uses software countermeasures and management procedures to protect itself against the threat of malicious software and unwanted programs. This includes viruses, spyware and trojan horses. The possibility of malware infection is a real and serious threat.

Antivirus software is installed on computers and laptops to mitigate against the risk of malware. However, it is important to always exercise caution, particularly when receiving e-mail attachments, opening links or visiting unfamiliar websites.

The instillation of illegal copies of software on any computer device is forbidden. Likewise, the installation of legal copies of a school purchased software on school staff's own equipment at home is not permitted.

In the event of a malware infection being detected or suspected, the following procedure must be followed:

- notify Cynnal and the Isle of Anglesey County Council IT Service Helpdesk immediately. Cynnal will attempt to establish the source of the virus and the authority's IT Service Desk will inform partner organisations and internal users;
- any affected devices will be physically disconnected from any network to which they are connected to;
- all removable devices connected to the affected device will be suitably checked for the presence of infection.

13. Storage Security

Personal information must be stored in a secure location with access only available to authorised persons who need access to that particular personal information. All personal information must be protected and kept secure in order to prevent loss, misuse or damage.

13.1. Paper Records

Personal information should be kept locked away whenever possible.

Any drawers, cupboards, cabinets, storage rooms or storage containers should be robust and locked when not in use.

Documents containing personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.

Documents should be kept in a safe and accessible location that is protected from flooding, dampness and other elements. Some documents may need to be kept in airtight containers to protect them from environmental damage.

In some circumstances, school records can be deposited with the Anglesey Archives for safekeeping. Please refer to the *Transferring School Records to the Anglesey Archives Policy.*

13.2. Electronic Records

If personal information is kept electronically, appropriate technical security measures need to be in place on all devices such as pseudonymisation, encryption or password protection.

Data will be regularly backed up in line with backup procedures.

14. Sharing Information Securely

There are various methods of sharing information securely. When sharing personal information, an appropriate and secure method should always be used.

If someone is requesting personal information, reasonable steps will be taken to verify the identity and address of the person making the request and whether they have the authority to request information.

The school is entitled to request relevant documentation to evidence that a person has the authority to request information and can ask for evidence of parental responsibility for a child if a parent is making a subject access request on behalf of a child.

The *Schools Data Subject Access Request Policy* should be followed in relation to requests from individuals for their personal information.

The school will follow the *Procedure for Sharing Information with Police Authorities in the United Kingdom (Gwynedd & Anglesey)* when dealing with requests from the Police.

14.1. By E-mail

School staff will only use an official, 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 and to share personal data.

When sending an e-mail that contains personal information, 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 possible to hover over the e-mail address to check further details regarding the recipient if it is an internal address and it may be appropriate to add photographs to internal e-mail accounts as an additional way of verifying the recipient.

If sending any e-mail to multiple recipients outside of the school, the blind copy facility (bcc) should be used so recipients can't view the e-mail addresses of other recipients.

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 and if they have a legitimate reason for receiving it.

E-mails containing personal and special category data must be identified using data classification terms (OFFICIAL or OFFICAL-SENSITIVE) within the subject field of the e-mail. Personal information should not be included in the subject field.

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

14.1.1. HWB E-mail Account- encryption

By default, HWB's email system is configured to encrypt its conversation with other email systems while sending and receiving messages. Users should be aware that this does not guarantee confidentiality of the message in certain circumstances, for example:

- the recipient's email system does not support encryption;
- the incorrect recipient email has been entered;
- the recipient forwards the email to an unauthorised person;
- the message is printed by the recipient

It is for these reasons that data sent externally which is classified as OFFICIAL-SENSITIVE should be encrypted. Please see guide- 'Encrypting email 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 not using encrypted e-mail, documents that contain personal information should be password protected with the password separately and securely shared with the intended recipient. Otherwise, personal information within the e-mail will need to be de-personalised (e.g. using initials or unique school identification numbers).

14.1.2. E-mail safety measures
All email received by the school will be passed through a security gateway before reaching user's mailboxes; if the email is flagged as a potential threat it will be quarantined or rejected by the system.

The following email safety settings are configured in the HWB tenancy:

- Safe Attachments: provides zero-day protection to safeguard your messaging system, by checking email attachments for malicious content. It routes all messages and attachments that do not have a virus/malware signature to a special environment, and then uses machine learning and analysis techniques to detect malicious intent. If no suspicious activity is found, the message is forwarded to the mailbox.
- Safe Links: provides time-of-click verification of URLs, for example, in emails messages and Office files. Protection is ongoing and applies across your messaging and Office environment. Links are scanned for each click: safe links remain accessible and malicious links are dynamically blocked.
- Safe Attachments for SharePoint, OneDrive, and Microsoft Teams: protects the school when users collaborate and share files, by identifying and blocking malicious files in team sites and document libraries;
- Anti-phishing: detects attempts to impersonate your users and internal or custom domains. It applies machine learning models and advanced impersonation-detection algorithms to avert phishing attacks. To learn more, see Configure anti-phishing policies in Microsoft Defender for Office 365;
- Anti-spam: protects the school's email from spam;
- Anti-malware: protect the school's email from malware.

14.2. By Post

If personal information is being sent by post, the information should be sealed within a robust envelope and the envelope should be marked using data classification terms (OFFICIAL or OFFICAL-SENSITIVE).

If the information contains special category data or is considered to be of a sensitive nature, the information should be sent by tracked mail or by a courier where appropriate. It may be appropriate to ask the recipient to confirm receipt. A record should be made of the date the information was sent and the method used.

Reliable transport couriers should be used at all times and packaging must be adequate to protect the contents from damage during transit.

14.3. By Telephone
If the school has received a request to share personal information via telephone, school staff must first confirm that the requestor is who they say they are and has a legitimate reason for access to the information. Confirmation is needed for both professionals and family members requesting information.

It may be appropriate to ask that a formal request is made in writing.

Once identity is confirmed, the school should only provide personal information to the person who has requested it. If they are unavailable, a message should be left for them to call back. A detailed (disclosure) message shall not be left with someone else or on a voicemail.

Care will always be taken when sharing personal information over the telephone of who might overhear the call. A record will be kept of any personal information that has been disclosed during a telephone call- this should include details around the date and time of disclosure, the reason for it and, if appropriate, who authorised the disclosure.

14.4. In Person
The most secure way of sharing personal information may be by delivering it in person. School staff can personally deliver personal information if this has been agreed by the Headteacher or other member of the senior management team.

A record should me made of any personal information that has been delivered in person; details of who has delivered it; the date and the reasons why.

Paper based personal information must be transported in a lockable box, sealed file or envelope marked with the appropriate data classification term (OFFICIAL or OFFICAL-SENSITIVE).

15. Transporting Information Securely

When there is a need to transport information held within documents, laptops, and mobile devices etc. which contain personal information, it is important to ensure precautions are taken to reduce the possibility of these being lost or stolen.

Personal information should only be transported when it is necessary. Personal information and mobile devices should not be transported where there is no absolute need to do so and only relevant documents should be transported where possible.

Information that may not be considered to be confidential can be dangerous in the wrong hands.

Personal information needs to be kept safe and secure, ensuring that information cannot be accessed by unauthorised persons. School staff should therefore take all reasonable steps to ensure security is maintained when transporting information between work and home or between work locations.

Documents and mobile devices should be transported in vehicles that are kept locked and secure particularly when unoccupied. Vehicles need to be secure and doors, windows, boot and sunroof should all be locked if personal information is within the vehicle.

Personal information or mobile devices should be transported within secure bags, boxes, folders etc. to reduce the risk of loss or damage and should be kept hidden away in a locked boot wherever possible or otherwise kept out of sight to discourage opportunist grab crimes.

Vehicles should be parked in busy, well-lit areas or where there is CCTV coverage to discourage thieves.

16. Secure Disposal of Personal Information

Personal information (and special category information) that is no longer required according to the *Schools Retention Schedule* will be deleted permanently from the school's information systems and any hard copies of personal information will be destroyed in a secure manner as soon as possible.

The school will follow the *Schools Retention Schedule* which sets out the relevant retention period for different types of personal information and documentation. The school needs to ensure that personal information is not kept for longer than necessary but also that personal information is not disposed of before the end of the retention period.

Personal information can be destroyed securely by using a cross-cutting shredder or via secure waste disposal arrangements. The school may use an appropriate third party to safely dispose of records on the school's behalf. If this is the case, the school will require the third party to provide sufficient guarantees that it complies with data protection law (e.g. Certificate of Destruction).

Personal data will not be left in an insecure location whilst in the process of being destroyed safely. Personal information shall not be disregarded via general waste, recycling or via a skip. A secure method **must** be used in all instances where there is personal data.

17. Secure Disposal of Redundant ICT Equipment

All redundant ICT equipment will be disposed of securely through the disposal scheme via Cynnal/the Council ICT Service. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data if appropriate.

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. The school's disposal record will include:

- date of disposal;
- authorisation for disposal, including whether any personal data is likely to be held on the storage media. If personal data is likely to be held, the storage media will either need to be over written multiple times to ensure the data is irretrievably destroyed or physically damaged by Cynnal/the ICT Service;
- how it was disposed of e.g. waste, including details of data cleansing;
- name of person and/or organisation who received the disposed item;
- copy of receipt of acceptance of responsibility for destruction of personal data where appropriate.

18. Legacy Systems

As well as being accepted good practice, PSN require that the school only uses software and hardware which is still maintained by the vendor so that if any security vulnerabilities are discovered in the technology, they may be "patched". Systems which are no longer maintained by their vendor are described as "Legacy Systems."

Using legacy software is considered by the Cabinet Office to be a security risk not only to the school and the Council, but to other organisations connected to the PSN and as such would result in failure of the annual PSN assessment.

It is for this reason that all legacy systems will be removed from the network once the vendor has withdrawn support. Where the data held in the legacy system must be retained, then it should be exported to a supported format, for example a newer version of the software.

19. Home Working

All data protection principles and policies apply when school staff work from home. The risk of data breaches occurring increases when personal information has been taken out of the school.

Staff should not take confidential or other information home without prior permission of the Headteacher, and only do so where satisfied appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. Any paper documents containing personal information should not be taken home unless it is **essential** to do so.

When a member of school staff has been given permission to take confidential or other information home, they must ensure that:

- a record is kept of any documents that contain personal information that have been taken home from school;
- the information is kept in a secure and locked environment (e.g. lockable cabinet) where it cannot be accessed by family members or visitors;
- computer screens are locked when not in use or left unattended and that all devices are password protected;
- the information cannot be inadvertently overlooked by family members or visitors;
- the information is not left unattended for any length of time, especially in a vehicle overnight;
- all sensitive material that requires disposal is shredded in the school, or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed. Personal information should not be disposed or destroyed at home.

Personal information should only be accessed via authorised electronic means that contain the required security measures. Staff should only use authorised electronic equipment from the school to access personal information. Personal information should not be saved on any personal devices and personal e-mail accounts should not be used to send or receive personal information.

Care should be taken when using free public wireless access as there is potential for passwords and data to be viewed by unauthorised persons.

Care should be taken that any telephone calls relating to school business or on-line learning sessions cannot be overheard by members of the family or visitors.

20. Data Processors

Where the school uses external organisations to process personal information on its behalf or uses “Cloud” storage suppliers (e.g. HWB- One Drive or Google Drive) or process personal information via external applications (apps), additional security arrangements need to be implemented in contracts and agreements with those organisations to safeguard the security of personal information. School staff should not use their own personal cloud storage arrangements for school related business.

The Schools Data Protection Officer will provide guidance to ensure that appropriate agreements and contracts (such as Data Processing Agreements) are in place with data processors to ensure appropriate information security procedures are in place. Such agreements and contracts will ensure commitment from data processors that they will meet the required security standards of the school.

Contracts and agreements with external organisations must provide that:

- the organisation may act only on the written instructions of the school;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the school and under a written contract;

- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist the school in meeting its obligations in relation to the security of processing; the notification of data breaches and Data Protection Impact Assessments (DPIAs);
- the organisation will delete or return all personal information to the school as requested at the end of the contract; and
- the organisation will submit to audits and inspections; provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it is asked to do something infringing data protection law.

Please refer to the *Schools Data Processing Policy* for more information and guidance.

21. Systems Implementation

The following security standards will be considered a minimum requirement when procuring new IT Systems:

- the system should require a complex password which is a minimum of 8 characters in length;
- the solution must be capable of forcing users to change their password after a given number of days, as determined by the system administrator;
- the solution must ensure that each user of the system have their own username;
- the system must prohibit re-use of passwords;
- the solution must disable user accounts after a predefined number of failed attempts set by the system administrator.

For new systems which are hosted external to the Council (in the “Cloud”) the supplier will be required to complete a Data Processing Agreement which commits them to meeting the required security standards of the Council, including (but not limited to):

- holding the data within the UK;
- enforcing password complexity;
- carrying out regular testing of security using third parties.

A full set of requirements is outlined in the IT Technical Specification included within the IT Procurement Policy. More information regarding Data Processing Agreements can be found under point 20 of this policy and by referring to the *Schools Data Processing Policy.*

22. Third Party Remote Access

It is common practice for third party IT suppliers to be provided with remote access to an organisation’s IT systems in order to provided technical support. In order to protect the security of data and ensure that suppliers meet the security standards required by the school and the Council, the following controls will apply:

- third parties will only be granted access upon completion of a Remote Access Agreement form which records their agreement to abide by Council IT policies as well as their commitment to a Data Processing Agreement;
- access will only be provided via the Council's secure web portal which offers an encrypted tunnel for communication and maintains an audit log of activity carried out by the supplier for later review if required;
- access from external sources is only permitted via peer to peer remote access systems such as TeamViewer, GotoMeeting where no other method is possible. Users are not permitted to set up unattended remote access. Access via this method must be entered in the school's remote access log for audit purposes;
- access will only be granted upon request to the IT Service Desk and will be revoked at the end of the working day. Where remote access is required with any urgency the request should be made via telephone, not email;
- no external third party (external contractors, partners, agents, the public or non-employee parties) may extract information from the School's IT equipment without explicit agreement from the Headteacher.

23. Data Breaches

A data breach is 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. This means that personal information has been compromised, damaged, lost or stolen.

A data breach can take many different forms, examples include, but are not limited to:

- accidental loss or theft of data or equipment on which personal information is stored e.g. information or IT equipment (laptops, tablets, mobile phones, devices containing personal data such as memory sticks);
- human error such as data shared with an unintended recipient via e-mailing information to an incorrect e-mail address; personal information being left in an insecure location; uploading personal information to a website or social media account;
- unauthorised access to or use of personal information either by a member of staff or third party including inappropriate access controls, resulting in compromised user accounts leading to unauthorised access to data;
- failure of equipment or IT systems (including hardware and software) resulting in loss of data or non-availability of data held on it;
- damage, destruction or loss of personal data; accidental or unlawful alteration or deletion of personal data (e.g. due to equipment failure or human error);
- loss of data or equipment through unforeseen natural events such as fire or flood;
- deliberate attacks on IT systems and cyber incidents such as hacking, viruses, phishing scams or malware infection;
- where information is obtained by deceiving a member of staff;
- breach of physical building access/security;
- unusual or uncontrolled system changes;
- inappropriate storage and/or disposal of IT equipment.

The school will contact the Schools Data Protection Officer to report **all** data breach incidents/'near misses' **as soon as possible.** The school will investigate any such breaches and will complete the required report of a data breach without undue delay. A data breach report template for schools and accompanying guidance is available on the Data Protection page on the Learning Service Microsite.

The school will need to take any necessary measures to address and mitigate the data breach and will take any remedial steps if necessary. The school will need to ensure that the information is gathered/returned and is destroyed straight away as a first step when the school becomes aware of the incident. The school will also review if it needs to undertake any required changes to current processes and/or practices to reduce the risk of the likelihood of a similar incident taking place again.

If the data breach is likely to result in a risk to the rights and freedoms of individuals, the school is required to report the data breach to the ICO, **within 72 hours** of becoming aware of the data breach. **It is the School's Data Protection Officer who makes the decision whether or not the breach needs to be reported to the ICO.**

The school will also need to notify the affected individuals without undue delay if a data breach is likely to result in a *high risk* to their rights and freedoms.

The school must keep a central record of all data breaches that will register all compliance failures. The Headteacher will ensure that a central record of all data breaches is kept via a *Data Breach Log*.

All staff need to be open about any incidents so that the school ensures that it acts responsibly, supports members of staff and deals with the breach as quickly and efficiently as possible. Not reporting an incident that should have been reported to the ICO, may have consequences for the school and for the individual member of staff.

The school will comply with the *Schools Data Breach Policy.*

24. Assessing Information Risk, Disaster Recovery and Business Continuity

The school is dedicated to the security of all information and ensures that all risks are identified. The school will ensure that the level of security and controls that are 'appropriate' to the risks presented by processing are implemented. Appropriate controls that are implemented are also documented (within a Risk Register where appropriate). A *Schools Data Protection Risk Matrix* and a *Schools Data Protection Risk Register* template are available on the Data Protection page on the Learning Service Microsite.

The school will regularly review the personal data that is held and the way it is used in order to assess how valuable, sensitive or confidential it is. The school will also assess the damage or distress that may be caused if the data was compromised.

Identified risks will feed in to *Data Protection Impact Assessments (DPIAs*) where necessary.

The school has a Disaster Recovery and Continuity Plan. This is in place to ensure that in the event of a physical or technical incident or failure of equipment or IT systems (including

hardware and software), availability and access to personal information can be restored in a timely manner to avoid the loss of data or non-availability of data.

Where possible, a general description of the school's technical and organisational security measures are included in the school's *Records of Processing Activities (ROPA).*

25. Checks and Audits

The Headteacher will conduct a data protection information security audit once every half-term. The findings of the audit will be shared periodically with the school governing body. It may be useful to also share findings with all school staff so that any lessons learned can be discussed and shared.

Any issues or concerns arising from the audit will need to be addressed by the school as soon as possible. The Schools Data Protection Officer can provide support with this.

A *Schools Data Protection Information Security Audit* template is available on the Data Protection page on the Learning Service Microsite.

26. Breach of the Policy

Non-compliance with this policy by members of school staff could lead to serious consequences including a breach of the law and a risk of significant civil and criminal sanctions for the individual and the school authorities.

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

Non-compliance by a member of staff may therefore be considered a disciplinary matter. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

27. Review of Policy and Oversight Arrangements

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

The policy will be approved by the Learning Service Senior Management Team 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.gov.uk

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/