Ysgol Cybi

Polisi Diogelu Data Ysgolion / *Schools Data Protection Policy*

(Fersiwn 3, Mai 2023 / *Version 3, May 2023*)

Ynglŷn â'r polisi hwn

Mae'r polisi hwn yn amlinellu'r hyn y mae'n rhaid i'r ysgol ei wneud i sicrhau bod gwybodaeth bersonol yn cael ei rheoli a'i hamddiffyn a'i bod yn sicrhau cydymffurfiad cyflawn â deddfwriaeth diogelu data.

Cefnogir y polisi hwn gan adnoddau ar dudalen 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 full compliance with data protection legislation.

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 Derbyniwyd gan Fwrdd o Lywodraethwyr / *Date Accepted by Board of Governors***
F1/*V1*	Rhagfyr 2020 / *December* 2020	Polisi newydd / *New policy.*	
F2/*V2*	Ebrill 2022 / *April 2022*	Adolygiad blynyddol o'r polisi / *Annual review of the policy*	

F3/*V3*	Mai 2023 / *May 2023*	Adolygiad blynyddol o'r polisi / *Annual review of the policy*	

Dyddiad yr adolygiad nesaf / *Date of next review*	
Bydd y polisi hwn yn cael ei adolygu yn: / *This policy will be reviewed in:*	Mai 2024 / *May 2024*
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.llyw.cymru

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@anglesey.gov.wales*

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'r *Ddeddf Diogelu Data 2018. / Policy template on the data protection legislation namely the* UK General Data Protection Regulation (UK GDPR*) and the* Data Protection Act 2018.

Cyfrifoldeb: / ***Responsibility:*** Cyfrifoldeb y llywodraethwyr ysgol a'r Pennaeth fel y rheolydd data yw sicrhau bod gweithdrefnau ar waith i sicrhau bod yr ysgol yn cydymffurfio â deddfwriaeth diogelu data. / *It is the responsibility of the school governors and the Headteacher as*

Content **Page**

1. Policy Statement

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

This policy sets out how the school complies with data protection obligations and seeks to protect personal information *(please see APPENDIX A for the relevant definition).* The school is fully committed to ensuring that personal information is properly managed and protected and that it ensures full compliance with data protection legislation.

Its purpose is also to ensure that all staff members understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access to in the course of their work. The school will ensure that it treats personal information lawfully and correctly.

The school will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so. The school will consult and seek the advice of the Schools Data Protection Officer relating to any issues, concerns or questions and before initiating any new data processing activities.

2. Scope

This policy applies to all employees, governors, contractors, agencies, representatives, and temporary staff working for and who process personal data on behalf of the school.

This policy applies to the personal information of job applicants, current and former staff, including employees, temporary and agency workers, governors, suppliers, volunteers, trainees/students, visitors, pupils, and parents/those with parental responsibility.

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, shared drive filing structure, e-mail, filing cabinet, shelves, and drawers).

The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments, staff development reviews and disciplinary records.

UK GDPR does not apply to deceased individuals as information about a deceased person does not constitute personal data and therefore is not subject to the *UK GDPR.*

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).

The school will also refer to other relevant internal policies and guidance which contain further information regarding the protection of personal information in other contexts, including:

- *Schools Information Security 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.*
- *Transferring School Records to the Anglesey Archives Policy.*
- *Schools Data Protection Impact Assessment Policy.*
- *School Staff E-mail Policy.*
- *Schools CCTV Policy.*
- *Schools Record Management Policy.*
- *Schools E-Safety Policy.*
- *School Staff Social Media Policy.*
- *Taking Photos for the Purpose of School Publicity Policy.*
- *Schools Retention Schedule*.

These are all available on the Data Protection Page on the Learning Service Microsite.

4. Responsibilities

The protection of personal data is everybody's responsibility. All staff members must ensure that they are committed to complying with data protection obligations.

The *UK GDPR* and *Data Protection Act 2018* require schools to 'demonstrate' compliance with legislation.

Schools will need to evidence compliance to meet the overarching principle of accountability.

It is the school as the data controller that has the ultimate responsibility for complying with data protection legislation. This responsibility cannot be delegated to the Local Authority, nor can it be delegated to the Schools Data Protection Officer or any data processors.

4.1. School Governing Body

The school governing body has the responsibility for:

- ensuring that this policy has been formally adopted by the school.
- the school's overall compliance with *UK GDPR* and the *Data Protection Act 2018.*
- maintaining the strategic oversight of the school's compliance by requesting to see evidence of compliance and to undertake monitoring visits to the school.
- appointing a governor as a Data Protection Champion on the governing board.
- regularly discussing data protection issues and matters at governing board meetings.
- monitoring the identified data protection risks of the school and to monitor actions that are in place to mitigate these risks.
- undertaking data protection training offered.

4.2. 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 compliance with *UK GDPR* and the *Data Protection Act 2018* within the day-to-day activities of the school.
- being the representative of the school as the data controller.
- ensuring and promoting understanding and compliance with this policy and other statutory and regulatory policies relating to data protection.
- regularly reviewing and keeping the school's *Information Asset Register* and *Records of Processing Activities (ROPA)* up to date.
- ensuring information assets and risks within the school are managed.
- ensuring that the school has registered and paid the annual data protection fee to the ICO.
- conducting internal audits that monitor compliance.
- ensuring that relevant information and support is provided regarding data subject access requests so that requests are processed within one calendar month.
- establishing a reporting and learning culture to allow the school to establish where problems exist and to develop strategies with the Schools Data Protection Officer to prevent future problems occurring.
- working with, and is the key link, between the school and the Schools Data Protection Officer in ensuring that the school is complying with its data protection obligations.

The school may appoint a member of staff to be the person who is ***responsible*** for data protection within the school who will deal with the day-to-day tasks and responsibilities for data protection but will ***not*** take on the **statutory responsibilities** of a **Data Protection Officer** (as this role has a legal status). This legal responsibility will remain with the Schools Data Protection Officer.

4.3. All Staff within the School

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

- complying both on an individual and collective basis with the *UK GDPR* and the *Data Protection Act 2018* within the day-to-day activities of the school.
- ensuring personal information is kept and processed in line with the *UK GDPR* and the *Data Protection Act 2018*.
- informing the Headteacher and/or the person responsible for data protection within the school immediately of any incidents, concerns, requests, and breaches relating to data protection.
- informing the Headteacher of any changes to personal details to help the school to keep personal information regarding staff up to date.
- ensuring understanding and compliance with this policy.
- ensuring understanding and compliance with all policies relating to data protection and security.
- adopting good practice standards relating to data protection.
- undertaking all data protection training offered.

4.4. Schools Data Protection Officer

The Schools Data Protection Officer is responsible for:

- informing and advising schools on their data protection obligations.
- monitoring compliance and performance against obligations, including conducting data protection compliance audits and reviews.
- providing advice, guidance, and recommendations on the impact of the school's data protection efforts and issues.
- providing an annual information governance assurance report to the school's governing body, and to provide a high-level annual summary report on all schools to the Learning Service Senior Management Team and the Isle of Anglesey County Council Governance and Audit Committee.
- creating and regularly reviewing data protection procedures, policies, guidance, and templates.
- facilitating and supporting the school to respond to data subject access requests within the time period.
- supporting and providing advice in the event of a data breach.
- checking and approving with third parties that handle the school's data, any contracts, or agreements regarding data processing.

- arranging and delivering data protection training for staff within schools including school governors.
- being the first point of contact for individuals whose data the school processes, and for the ICO.

The school should support the Schools Data Protection Officer to fulfil their role by ensuring that:

- the Schools Data Protection Officer is involved, closely and in a timely manner, in all data protection matters.
- the Schools Data Protection Officer reports to the highest management level of the school, i.e., School Governing Board level.
- the Schools Data Protection Officer operates independently from the school.
- the school gives the Schools Data Protection Officer appropriate access to personal data and processing activities.
- the school gives the Schools Data Protection Officer appropriate access to other services within the school so that they can receive essential support, input, or information.
- the school seeks the advice of the Schools Data Protection Officer when carrying out a DPIA; and
- the school records the details of the Schools Data Protection Officer as part of the school's records of processing activities.

The school as the data controller has the responsibility to comply with the *UK GDPR* and other data protection legislation. The Schools Data Protection Officer plays a crucial role in helping the school to fulfil the school's data protection obligations but cannot take responsibility for the school's data protection compliance.

5. Data Protection Principles

The school's approach to data protection will be, as required by *UK GDPR*, 'data protection by design and default' and 'privacy by design'. In essence, this means that the school needs to integrate data protection in to processing activities and business practices, from the design stage right through the lifecycle.

The school will comply with the following **six fundamental data protection principles** when processing personal information:

1. Personal information will be processed in a legal, fair, and transparent manner.
2. Personal information will be collected for specified, explicit and legitimate purposes only, and will not be processed in a way that is incompatible with those legitimate purposes.
3. Will only process personal information if it is adequate, relevant and is limited to what is necessary for the relevant purposes (data minimisation).

4. Personal information must be kept accurate and up to date, and reasonable steps will be taken to ensure that inaccurate personal information is deleted or corrected without delay.
5. Personal information will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed.
6. Personal information will be processed safely. Appropriate technical security measures will be taken to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

The school will review the purposes of the particular processing activity and select the most appropriate lawful basis (or bases) for that processing before the processing starts for the first time and then regularly while it continues. Please see section 9 for definitions of specific processing activities.

The school must have the ability to **demonstrate** compliance with these principles. If the school is unable to comply with all six principles, then data should **not** be processed.

6. Data Subject's Rights

Data protection legislation provides the following rights for individuals:

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erase.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Rights in relation to automated decision making and profiling.

The Schools Data Protection Officer will support the school with dealing with any requests from individuals to exercise any of their rights.

6.1. <u>The right to be informed</u>

Individuals have the right to know that information about them is being processed. The school will inform individuals at the point of collection, by a *Privacy Notice,* about how, why and on what basis that information is processed.

6.2. <u>The right of access</u>

Individuals have the right to obtain confirmation that their information is being processed and to also request access and to have copies of personal information that the school holds about them or information about a child they are responsible for (subject access request-SAR).

A subject access request can be made verbally or in writing, but it needs to be sufficiently clear what personal information is being requested.

Before responding to a subject access request, reasonable steps will be taken to verify the identity of the person making the request and whether they have the authority to request information on behalf of another individual. It is possible to ask for additional information to confirm identity and it is possible to ask to see identity documents such as a driving licence or passport that will verify the identity of the individual.

Once a data subject access request is received, the information requested must be provided without delay and at the latest within **one calendar month** of receiving the request. If a data subject access request is complex (i.e., if a request is manifestly unfounded or excessive, or data is required from more than one source or the data subject has made numerous requests (whether current or not)), the response period can be extended by up to a further two months. The applicant will be informed if the response timeframe will be extended and the reasons why. It is expected that the school responds within the time period irrespective if school term breaks occur during the response period. The school will notify pupils and parents/those with parental responsibility that there is limited access to requests during the school term breaks but will still deal with the requests within the response period.

There are limited timescales within which to respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

In certain circumstances the school may be exempt from providing some or all of the personal data requested. Exemptions should only be applied on a case-by-case basis after careful consideration of all the facts. The Schools Data Protection Officer will provide advice and guidance on what information can and cannot be shared.

The school will gather and collate all the personal data that has been requested. The school will need to gather all electronic and paper records that includes personal data within files, e-mails, CCTV, letters, reports, and images.

No fee can be charged by the school for dealing with subject access requests. However, if a request is unfounded, excessive and has been submitted previously, the school has a right to charge a ‘reasonable’ administrative fee. The Schools Data Protection Officer can provide guidance on what is considered to be a ‘reasonable fee’.

The Schools Data Protection Officer will provide figures regarding the number of subject access requests in the annual information governance assurance report to the school’s governing body. Figures will also be included in the Schools Data Protection Officer’s high level annual summary report on all schools that is presented to the Learning Service Senior Management Team and the Isle of Anglesey County Council Governance and Audit Committee.

The school will follow the *Schools Subject Access Request Policy* on how to deal with subject access requests that is available on the Data Protection page on the Learning Service Microsite.

6.3. The right to rectification

Individuals have the right to have their personal data corrected if it is inaccurate or incomplete. The school will rectify the personal data as soon as possible and will do so within one calendar month of receiving the request to rectification. This can be extended by a further two months where the request to rectification is complex. A note should be made on relevant records if there is doubt regarding accuracy whilst dealing with the request.

It may be possible that the school may not be able to change or delete the personal information on every occasion, but anything that is factually incorrect should be corrected.

Where the school will not be taking any action in response to the request to rectification, the school will explain the reasons why to the individual and will inform them of their right to complain to the ICO. The school will also make a record of this.

6.4. The right to erase

Individuals have the right to request that any personal information held on them is deleted or removed if the data is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing. This right is also known as the right to be forgotten.

An erasure request can only be refused if an exemption applies, but it is likely an exemption will apply in the context of erasing school records. The school will consider every request on an individual basis. The school will respond to the request to erasure within one calendar month.

The school may refuse a request to erase personal data:

- where the school needs to comply with a legal obligation (to keep the data).
- for protecting an individual's vital interests or for tasks carried out in the public interest.
- when archiving in relation to public interest, scientific/historical research, or statistical purposes.
- when the personal data is required for the exercise of legal claims.
- when the processing is necessary for exercising the right of freedom of expression and information.

The school will inform third parties that also process the personal data unless it involves a disproportionate effort to do so.

6.5. The right to restrict processing

Individuals are entitled to block the processing of their personal data in certain circumstances. The data may continue to be stored but processing of it must cease.

Individuals have the right to restrict the processing of their personal data where:

- the accuracy of the information is contested.
- the processing is unlawful (but they do not want the data to be erased, but restricted instead); or
- the school no longer needs the personal information, but they require the data to establish, exercise or defend a legal claim.

Individuals also have the right to restrict the processing of personal information temporarily where:

- they do think it is accurate (and the school is verifying whether it is accurate).
- they have objected to the processing (and the school is considering whether the school's legitimate grounds override their interests).

The school will need to inform any third party that has received the data of the need to limit processing, and to inform the individual of the identity of these third parties. The school will inform individuals when the school decides to lift a restriction on processing.

6.6. The right to data portability

Individuals have the right to request that they receive a copy of their personal data in a structured format. Requests should be processed within one calendar month, provided there is no undue burden, and it does not compromise the privacy of other individuals. Individuals can also request that their personal data is transferred directly to another system. No fee can be charged for this. The right to data portability only applies:

- to personal data an individual has provided to the school as the data controller.
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

6.7. The right to object

Individuals have the right to object to their personal information being processed if the school is:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

The school will comply with the request unless there are strong, lawful reasons for processing or there is a need to establish, exercise or defend legal claims.

6.8. Rights in relation to automated decision making and profiling
Data Protection legislation allows:

- Automated individual decision-making- making a decision solely by automated means without any human involvement; and
- Profiling- automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.

The school has a right to carry out automated decision making and profiling only if:

- the processing is necessary for entering into, or performance of, a contract.
- the processing has been authorised by member state law that includes measures to safeguard data subjects' rights; or
- the processing is based on explicit consent.

There are additional rules to protect individuals if automated decision making and profiling have legal effects or similarly significantly affects them. The school must ensure that individuals are able to:

- obtain human intervention.
- express their point of view; and
- obtain an explanation of the decision and to challenge it.

The school will not carry out automated decision making, including profiling, based on any individual's sensitive personal information.

6.9. Other rights
Additional to the rights above, individuals also have the right to:

- withdraw their consent to processing at any time.
- make a complaint to the ICO.

7. Children's Rights

Children have the same rights as adults over their personal information which they can exercise as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.

In Wales there is no set age at which a child is generally considered to be competent to provide their own consent to processing. Competence is assessed depending upon the level of understanding of the child. If a child is competent then, just like an adult, they may authorise someone else to act on their behalf. This could be a

parent/those with parental responsibility, another adult, or a representative such as a child advocacy service, charity, or solicitor.

In the UK only children aged 13 or over are able provide their own consent for information society services (ISS). ISS generally includes websites, apps, search engines, online marketplaces, and online content services such as on-demand music, gaming and video services and downloads.

The school will ensure that it and its data processors (as far as is practicable) comply with the Children's Code (age-appropriate design code) which is a data protection code of practice if providing online services, such as apps, online games, and web and social media sites that are accessed by children.

8. Parent's Rights

A person with parental responsibility can exercise rights on behalf of a child if:

- the child authorises them to do so.
- when the child does not have sufficient understanding to exercise the rights him or herself; or
- when it is evident that this is in the best interests of the child.

A person with parental responsibility is someone who, according to the law in the child's country of residence, has the legal rights and responsibilities for a child that are normally afforded to parents. This will not always be a child's 'natural parents' and parental responsibility can be held by more than one natural or legal person.

The school must verify that the person giving consent does, in fact, hold parental responsibility for the child. The school is entitled to request relevant documentation to evidence this as well as the identity of the person making any requests on behalf of the child.

In addition, parents have their own independent right under *The Education (Pupil Information) (Wales) Regulations 2004* to access the official education records of their children who attend a maintained school. Parents can make requests in writing to the Headteacher. Pupils can also make a request for their own education record. A request for an educational record must receive a response from the school within 15 school days. The school may withhold information in certain circumstances, such as where serious harm may be caused to the pupil's physical or mental health or another individual, or where the request is for an exam script or for exam marks before they are officially announced. The school can charge an amount for information provided from an education record dependent upon the number of pages provided.

9. Conditions for Processing (Legal Basis)

9.1. Article 6

Personal data must be processed fairly and lawfully in accordance with the individual's rights. The school, as the data controller, will only process personal

information where at least one of the conditions of *Article 6 of UK GDPR* has been satisfied:

- 6(1)(a)- **individual's consent-** the individual has given clear consent for the school to process their personal data for a specific purpose.
- 6(1)(b)- **processing is necessary for a contract-** the processing is necessary for a contract with the individual, or because they have asked to take specific steps before entering into a contract.
- 6(1)(c)- **processing is necessary to comply with a legal duty-** the processing is necessary for the school to comply with the law (not including contractual obligations).
- 6(1)(d)- **processing is necessary for the individual's vital interests or another natural person-** the processing is necessary to protect someone's life.
- 6(1)(e)- **processing is necessary as it undertakes a task in the public interest or exercise of official authority-** the processing is necessary for the school to perform a task in the public interest or for the school's official functions, and the task or function has a clear basis in law.
- 6(1)(f)- **processing is necessary for the purposes of legitimate interests of the data controller or third party-** the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests *(this does not apply to public authorities processing data to perform official tasks*).

The school will document its decision as to which lawful basis applies within its *Records of Processing Activities (ROPA),* to help demonstrate compliance with the data protection principles. The school will include information about both the purposes of the processing and the lawful basis for it in the school's *Privacy Notice.*

9.2. Article 9

The lawful basis for processing **special category data** requires that in addition to satisfying at least one of the conditions of *Article 6 of UK GDPR*, a condition in *Article 9 of UK GDPR* must also be satisfied *(please see section 10 for definitions of special category data).* The school, as the data controller, will only process sensitive personal information if a condition in *Article 9* has been met:

- 9(2)(a)- **processing with the specific and explicit consent of the individual-** unless reliance on consent is prohibited by EU or Member State law.
- 9(2)(b)- **processing is necessary under employment law-** or social security or social protection law, or a collective agreement.
- 9(2)(c)- **processing is necessary to protect the individual's vital interests-** of a data subject who is physically or legally incapable of giving consent.

- 9(2)(d)- **processing for the use of a special category group (not-for-profit organisation with a political or religious aim or trade union).**
- 9(2)(e)- **processing relates to information made public by the individual.**
- 9(2)(f)- **processing is necessary so that the establishment can defend legal claims-** or where the courts are acting in their judicial capacity.
- 9(2)(g)- **processing is necessary for reasons of substantial public interests based on law-** which is proportionate to the aim pursued and which contains appropriate safeguarding measures- this means that Member States can extend the circumstances where sensitive data can be processed in the public interest.
- 9(2)(h)- **processing is necessary to respond to the needs of Occupational Health and Social Care-** necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union Member State law or a contract with a health professional.
- 9(2)(i)- **processing is necessary for Public Health reasons-** such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- 9(2)(j)- **processing is necessary for archiving purposes in the public interest; or for scientific or historical research purposes; or for statistical purposes.**

Further special category conditions are included in *Schedule 1* of the *Data Protection Act 2018.*

The school will not process sensitive personal information until the individual has been properly informed (by way of a *Privacy Notice* or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Where criminal offence information is processed, the school will identify a lawful condition for processing that information and will document this.

The school will document its decision as to which lawful basis applies within its *Records of Processing Activities (ROPA).*

The school will notify the Schools Data Protection Officer before processing any sensitive personal information, in order that the Schools Data Protection Officer may assess whether the processing complies with the criteria noted above.

10. Special Categories of Personal Data

Special categories of personal data are sometimes referred to as sensitive personal information or sensitive personal data. These are considered to be more sensitive and may only be processed in more limited circumstances.

The *UK GDPR* defines special category data as:

- personal data revealing racial or ethnic origin.
- personal data revealing political opinions.
- personal data revealing religious or philosophical beliefs.
- personal data revealing trade union membership.
- genetic data.
- biometric data (where used for identification purposes).
- data concerning health.
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Further to section 9.2, the school must determine the condition for processing special category data before beginning to process the information and will document the condition.

The school will not share any medical information regarding a pupil unless there is a legal basis in doing so. The school may put practices in place to share medical information with the consent of the pupil/parent/those with parental responsibility if it is felt that there is a need to specifically share the information in order to protect the health and well-being of the particular pupil (e.g., a notice on a noticeboard in a restricted access staff room that contains personal and sensitive information of a pupil with a severe food allergy). In such circumstances, the school will seek advice from the Schools Data Protection Officer and the health and well-being risks posed, and the need to keep sensitive personal information safe, will have to be balanced against each other.

11. Consent

Consent may be used by the school as a legal basis for processing if it is the most appropriate legal basis to be used or if another lawful basis is not appropriate.

Consent must be a positive action, so individuals must always opt-in and take an affirmative action in providing their consent. The school will require consent to be provided for every separate processing activity.

The school will keep a record of consent via a register that lists everyone who has or has not provided consent and for which specific processing activity. The school will ensure that this is kept accurate and up to date and that there is a process in place for ensuring that the school complies with the consent decisions recorded.

Consent must be freely given, and it must be as easy to withdraw as it is to give. Individuals have the right to withdraw consent at any time and the school will up-date the record of consent to reflect any changes.

If the school has not received a consent form or no other positive action to provide consent has been provided, the school will take this as no consent being provided and will document and action this.

Consent forms are available on the Data Protection page on the Learning Service Microsite.

12. Accuracy and Relevance

The school will ensure that any personal information that is processed is accurate, up to date, relevant, adequate, and not excessive (proportionate) and is processed for the purpose for which it was obtained. Personal data obtained for one purpose will not be processed for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

The school will make it clear that individuals must take reasonable steps to ensure that personal data that the school holds about them is accurate and is up-dated as required. This is included in the school's *Privacy Notice* and the school will confirm at regular intervals that the information held is correct, in particular addresses and contact details. The school will up-date the information as soon as possible both in paper and in electronic records.

13. Retention of Personal Information

Personal information (and special category information) will be kept securely in accordance with the *Schools Retention Schedule* which is available on the Data Protection page on the Learning Service Microsite.

Personal information (and special category information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend on the circumstances, including the reasons why the personal information was obtained. The school should follow the *Schools Retention Schedule* which sets out the relevant retention period for different types of personal information and documentation. Where there is any uncertainty, the school should consult with the Schools Data Protection Officer for guidance.

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.

14. Data Recording

The school will keep records in such a way that the individual concerned can inspect them. The information may also be inspected by the courts or any legal official at some point in the future. It should therefore be correct, unbiased, unambiguous, and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

15. Records of Processing Activities (ROPA)

The school will keep written records of processing activities as required by data protection legislation, including:

- the name and details of the school; contact details of the Schools Data Protection Officer and any other joint data controllers if applicable.
- the purposes of the processing.
- a description of the categories of individuals and categories of personal data processed.
- categories of recipients of personal data.
- where possible, the retention schedules for the different categories of personal data.
- where possible, a general description of technical and organisational security measures.

The school will also, as part of the record of processing activities, document or provide a link to documentation on:

- information required for *Privacy Notices*.
- records of consent.
- controller-processor contracts.
- the location of personal data.
- Data Protection Impact Assessments (DPIAs).
- personal data breaches.
- special category data or criminal conviction and offence data.

If the school processes special category data or criminal conviction and offence data, written records will be kept of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose.
- the lawful basis for processing; and
- whether the school retains and erases the personal information in accordance with the policy document and, if not, the reasons for not following the policy.

The school will conduct regular reviews of the personal information that is processed and up-date documentation accordingly. This may include:

- carrying out information audits to find out what personal information the school holds.
- creating data map flows for different information processes.
- distributing questionnaires and talking to all staff within the school to get a complete picture of the school's processing activities; and
- reviewing policies, procedures, contracts, and agreements to address areas such as retention, security, and data sharing.

The school will document processing activities in electronic format so that information can be added, removed, and amended easily so that the record of processing activities is kept accurate and up to date.

A template for *Records of Processing Activities* and accompanying guidance is available on the Data Protection page on the Learning Service Microsite. The school as a data controller **must** keep a *Records of Processing Activities*.

The school will comply with the *Schools Records Management Policy.*

16. Disclosure and Sharing of Information

Data protection law does not prevent, and is not a barrier, to sharing information but rather provides a framework to ensure that personal information is shared lawfully and in an appropriate and safe way. However, it is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- other staff members on a *need-to-know* basis.
- relevant parents/those with parental responsibility.
- other organisations if it is necessary in the public interest e.g., prevention of crime.
- other authorities such as the Local Education Authority and schools to which a pupil may move, where there are legal requirements.
- organisations that collaborate with the school (such as Social Services *(please see section 16.2)*) or that are part of an Information Sharing Protocol (ISP).

When sharing personal information, the school will ensure that:

- it is allowed to share the personal information.
- the information is shared only with the people who *need* to have it.
- adequate security (taking in to account the nature of the information) is in place to protect the information and to ensure that it is shared safely.
- it will provide an outline in a *Privacy Notice* of who receives personal information from the school.
- the information is accurate and up to date.
- the information is shared in a timely fashion.

Individual staff members will only access information that they have the authority to access, and only for authorised purposes and will only allow other school staff to access personal information if they have the appropriate authorisation.

Decisions on whether to share information must be taken on a case-by-case basis. The school will base its decisions around sharing information on considerations of the safety and well-being of the individual and others who may be affected. The school will not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else.

Personal information should not be disclosed without establishing the identity of the recipient. Information should not be provided to other parties, even if they are related (e.g., in the case of divorced parents, it is important that information regarding one party is not given to the other party who which he/she is not entitled). The school will keep a record of the decision to share information or not and will explain the reasons behind the decision. If the school has shared information, a record will be kept on what personal information has been shared, with whom it has been shared and for what purpose.

Any personal data passed to a third party for processing (namely an external company) will be covered by a Data Processing Agreement (DPA). A Data Processing Agreement is needed when the school as the data controller asks a data processor to process data on behalf of the school.

The school will sign up to the Wales Accord on the Sharing of Personal Information (WASPI). This is a tool to help share personal information effectively and lawfully on a multi-agency basis within Wales.

If the school regularly shares information with an agency or organisation, there may be a need for an Information Sharing Protocol (ISP) or a Data Disclosure Agreement (DDA) depending on the type of information sharing.

The school may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any pupils or staff members.

The school should contact the Schools Data Protection Officer for advice if the school is in any doubt if personal information should be shared or not with agencies and third parties requesting information.

16.1. Request from Third Parties for an Individual's Personal Information
The school may receive requests from other agencies or third parties such as the Police, DWP, solicitors etc. to physically access or receive a copy of the personal information relating to an individual.

The school will share personal data with law enforcement and government bodies where it is legally required to do so, including for:

- the prevention or detection of crime and/or fraud.
- the apprehension or prosecution of offenders.
- the assessment or collection of tax owed to HMRC.
- in connection with legal proceedings.
- where the disclosure is required to satisfy safeguarding obligations.
- research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

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

16.2. Protection of Children and Vulnerable Adults

The *UK GDPR* and *Data Protection Act 2018* do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.

Relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional, or mental harm, or if it is protecting their physical, mental, or emotional well-being. The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child.

Fears about sharing information should not be a barrier to safeguarding and promoting the well-being of children at risk of abuse or neglect.

The school will need to follow safeguarding policies and procedures without delay regarding what personal information can be shared with the relevant authorities such as Children & Families Services, Adult Services, or the Police if there are any concerns that a child or vulnerable adult may be at risk of serious or significant harm.

In some circumstances, the duty of protecting the confidentiality of personal information must be overridden, when there is a duty to protect children or vulnerable adults who are at risk of serious harm. In such circumstances, the school will seek advice from the Schools Data Protection Officer. The risk posed and the individual's right to privacy will have to be balanced against each other.

If unsure of what information can be shared, please discuss with the Schools Data Protection Officer.

For more information regarding sharing information to safeguard children, please refer to the *Welsh Government's document- Social Services and Well-being (Wales) Act 2014, Working Together to Safeguard People, Information sharing to safeguard children, Non-statutory guide for practitioners,* July 2019 which is available on the Data Protection page on the Learning Service Microsite.

17. Freedom of Information Requests

The *Freedom of Information Act 2000* creates a general right of access to all types of recorded information held by public authorities. This includes electronic and paper records, photographs, and recordings.

The general public has the right to be informed whether a public body holds certain information and the right to have that information communicated to them.

The law gives individuals the right to access information that is already held. There is no obligation for the school to create information or provide explanations or advice.

The school has 20 working days to respond to a request. For a request to be valid under the *Freedom of Information Act* it must be in writing (please note that public authorities also have duties under equalities legislation- the school may need to provide additional support or reasonable adjustments to allow an individual to make a request where needed).

The *Freedom of Information Act* contains a number of exemptions that allows the school to withhold information from a requester. Some exemptions relate to a particular type of information and other exemptions are based on the harm that would arise or would be likely arise from disclosure. There is also an exemption for personal data if releasing it would be contrary to the *UK GDPR* or the *Data Protection Act 2018.*

The school can refuse an entire request under the following circumstances:

- it would cost too much or take too much staff time to deal with the request.
- the request is vexatious.
- the request repeats a previous request from the same person.

If the school is refusing all or any part of a request, the school must send the requester a written refusal notice.

The Schools Data Protection Officer can provide advice and guidance to the school regarding dealing with freedom of information requests.

There are resources available on dealing with freedom of information requests on the Data Protection page on the Learning Service Microsite including an *Access to Information Guidance* and an *Access to Information Chart.*

17.1 Publication Scheme

The school is also obliged to proactively publish certain information about its activities. The *Freedom of Information Act* requires every public authority to have a publication scheme, approved by the ICO, and to publish information covered by the scheme. The Act is designed to increase transparency and members of the public should be able to routinely access information that is in the public interest and is safe to disclose.

The scheme must set out the school's commitment to make certain classes of information routinely available, such as policies and procedures, minutes of meetings, annual reports, and financial information.

Some types of information do not fall under the scheme including information that is in draft form; information that has been archived or it is difficult to access; information that is exempt from disclosure under the Act and part of the document is exempt from disclosure and it would not be practical to publish the information in a redacted (edited) form.

The school's publication scheme should be made available via the school website. If the school does not have a website, the school must still list the information in the school's guide to information and give contact details so people can make a request to see it.

The school will maintain its publication scheme and continue to publish the information it lists. The school has a process in place to:

- review what information the school is publishing.
- ensure the school makes newly created information that falls within the scope of the scheme available promptly; and
- replace or update information that has been superseded.

A publication scheme template is available on the Data Protection page on the Learning Service Microsite. The Schools Data Protection Officer can provide advice and guidance to the school regarding what to include in the publication scheme.

18. 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:

- 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.

The school must keep a central record of all data breaches that will register all compliance failures. Figures regarding the number of data breaches will be included in the annual information governance assurance report to the school's governing body. Figures will also be included in the Schools Data Protection Officer's high level annual summary report on all schools that is presented to the Learning Service Senior Management Team and the Isle of Anglesey County Council Governance and Audit Committee.

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 Schools 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.

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*.

19. Sharing Data Protection Concerns

Staff within the school should inform the Headteacher/person who is responsible for data protection within the school, and if appropriate, the Schools Data Protection Officer, if they have any concerns or suspects that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the legal conditions in *Article 9* being met.
- access to personal information without the proper authorisation.
- personal information not kept or deleted/destroyed securely.
- removal of personal information, or devices containing personal information (or which can be used to access it), from the school's premises without appropriate security measures being in place.
- any other breach of this policy or of any of the data protection principles set out in section 5.

20. Information Asset Register

The Headteacher will need to ensure that an *Information Asset Register* is in place and that it is reviewed on a regular basis. The information asset register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

An *Information Asset Register* template and *Information Asset Register Guidance* are available on the Data Protection Page on the Learning Service Microsite.

21. Privacy Notice

The school has a Privacy Notice in place that informs individuals about the personal information that is collected and is held about them and how they can expect their personal information to be used and for what purposes. The Privacy Notice must be specific to the activity which requires personal information. This must happen at the time that the information first starts to be gathered on an individual.

Whenever information is collected about individuals, the school will provide the following information so that the school is transparent and provides accessible information about how personal data is used:

- the identity and contact details of the school as the data controller.
- the purpose that the information is being collected for.
- the lawful basis for collecting the information.
- any other purposes that it may be used for.
- how the information is collected.
- with whom the information will or may be shared with (any third parties).
- how long the information is kept.
- details about the rights of individuals (e.g., the rights of access to personal data that is being held by the school).
- details about the Schools Data Protection Officer.

Appropriate measures are taken to provide information in the Privacy Notice in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. If information is directly collected from a child, the Privacy Notice must be age appropriate.

The Privacy Notice will be shared via the school website; social media accounts and will be made available in hard copy upon request.

A summary of the Privacy Notice will be included within all documents that collect personal information and within consent forms.

Privacy Notice templates for parents and pupils (general); a children and young people's version and a version for the school workforce, are available on the Data Protection page on the Learning Service Microsite.

22. Data Protection Impact Assessments (DPIAs)

Where processing is likely to result in a high risk to an individual's rights and freedoms (e.g., where the school is planning to use a new form of technology), before commencing the processing, a DPIA will be performed to assess the following:

- whether the processing is necessary and proportionate in relation to its purpose.
- the risks to individuals.
- what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the school should therefore contact the Schools Data Protection Officer in order that a DPIA can be undertaken.

During the course of any DPIA, the school will seek the views of any representative group and any other relevant stakeholders (where applicable).

DPIAs are a legal requirement for processing activities that are likely to be high risk. A DPIA should be considered as an on-going process with regular reviews based on the level of risk and the nature of the processing activity.

A *Schools Data Protection Impact Assessment (DPIA) Policy* and template as well as 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.

23. Information Security

23.1. School
The school will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

The school will ensure:

- that where possible, personal information is pseudonymised or encrypted.
- the on-going confidentiality, integrity, availability and resilience of processing systems and services.
- that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner.
- that a process is in place for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- that there are appropriate secure spaces 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.
- that all personal and special categories data stored on the school's IT systems must be identified using data classification terms (OFFICIAL or OFFICAL-SENSITIVE).

The school will comply with the *Schools Information Security Policy.*

23.2. External Organisations

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts and agreements with those organisations to safeguard the security of personal information. **The school must have an official contract or agreement in place with any data processors that process data on behalf 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.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or existing agreement is altered, the school must seek approval of its terms by the Schools Data Protection Officer. The Schools Data Protection Officer will ensure that there are clearly defined agreements in place between the school and the organisation to ensure that data is suitably protected and provides clarity on roles and responsibilities.

24. Secure Storage of Personal Information

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.

24.1. Paper Records

Personal information should always be kept locked away. 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.

Particular care should be taken if documents have to be taken out of the school building. Documents including personal information should not be removed from the school's premises unless appropriate security measures are in place to secure the information.

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.

Blinds on ground floor windows should be closed at the end of the day.

24.2. 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.

All electronic devices that contain personal information need to be password protected with access only provided to authorised persons.

Strong passwords need to be in place which contain at least eight characters; a mix of upper- and lower-case characters and a mix of numbers and letters. 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.

All computer and laptop screens will automatically lock after a certain period and staff will also physically lock their screens if leaving their desks for a period of time.

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

All portable electronic devices should be kept as securely as possible. If they contain personal information, they should be kept under lock and key when not in use.

Encryption software should be used to protect all portable devices and removable media, such as USB devices (memory sticks or another form of memory storage not part of the computer itself) which hold personal information. Staff members should not remove devices containing personal information (or which can be used to access it), from the school's premises unless appropriate security measures are in place to secure information and the device.

The use of removable media devices is not encouraged when there are alternative technologies available that do not require physically transferring data between locations. The school will move away from using these kinds of devices for storing personal information wherever possible.

Staff members will not use personal devices or drives (such as mobile phones) to store or share personal information relating to school and work business.

25. 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.

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 discarded via general waste, recycling or via a skip. A secure method **must** be used in all instances where there is personal data.

26. Annual Data Protection Fee

Schools, like every organisation or sole trader who processes personal information, are required under the *Data Protection (Charges and Information) Regulations 2018*, to pay an annual data protection fee to the ICO, unless they are exempt**. All schools are required to pay the annual data protection fee.** Failure to do so will result in a fixed penalty**.** The school will register as a public body.

Registration details are added to the data protection public register that can be viewed on the ICO website. The school has a unique registration number. Contact details for the Schools Data Protection Officer is included against the school's registration details.

27. Photographs and Images

As part of school activities, photographs and images will be taken of individuals within the school. Photographs and images taken for official school use that may be used for communication, marketing and promotional materials will be covered under *UK GDPR* and *Data Protection Act 2018* and the school will need to inform pupils why they are being taken and what they will be used for.

A consent form is available on the Data Protection page on the Learning Service Microsite that is to be used in order to obtain consent by pupils/parents/those with parental responsibility regarding where the photographs and images will be published. Consent will be provided on different elements of where photographs and images can be shared and used such as on the school website, social media accounts, newspapers, brochures, newsletters, and apps.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the school will delete the photograph or video and not distribute it further.

The school can share the *Taking and Using Photographs or Videos of Your Child at School: Your Rights* leaflet with parents that is available on the Data Protection page on the Learning Service Microsite.

The school will comply with the *Taking Photos for the Purpose of School Publicity Policy.*

28. Website and Social Media

The school will obtain written consent for sharing personal information regarding pupils on its website and social media accounts, including photographs and images. Pupils, parents/those with parental responsibility will be informed about the consequences of personal data being disseminated worldwide.

A consent form is available on the Data Protection page on the Learning Service Microsite that is to be used in order to obtain consent by pupils/parents/those with parental responsibility regarding what information, photographs and images will be published on any websites and social media accounts.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the school will take every reasonable step to delete/remove the information/photograph/image from the website and/or social media accounts to stop further distribution. However, it must be recognised as the personal data is on a website and/or social media

accounts, the information may already have been viewed and shared beyond the school's control.

The school can share the *Taking and Using Photographs or Videos of Your Child at School: Your Rights* leaflet with parents that is available on the Data Protection page on the Learning Service Microsite.

The school will comply with the *Taking Photos for the Purpose of School Publicity Policy.*

29. 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 and to share personal data.

If a document that contains personal information has to be shared via e-mail, the document will be password protected with the password separately and securely shared with the intended recipient. Encryption should be used wherever possible to share personal information via e-mail.

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

The school will comply with the *Schools Staff E-mail Policy.*

30. CCTV (if relevant)

Capturing and/or recording images of identifiable individuals is an example of processing personal information and therefore needs to comply with *UK GDPR* and the *Data Protection Act 2018*. The school must also have a *CCTV Policy* in place.

Data Protection Impact Assessment (DPIA) needs to be completed when using CCTV or considering purchasing a surveillance system. The Schools Data Protection Officer will provide guidance and support with completing these.

The school must notify staff, pupils, and visitors why it is collecting personal information in the form of CCTV images. A sign notifying this must be in place within all zones that are being filmed. Using prominently placed signs at the entrance to the school and then using further signs inside the zones will let people know when they are in an area where a surveillance system is in operation.

The school will notify individuals within a *Privacy Notice* that the school uses CCTV.

The school will ensure that it has a set retention period based on the possible need to review the footage and will consider who is allowed access to this footage and why.

Individuals and law enforcement agencies will have the right to request access to the images. All such requests will be logged.

The school will follow *'In the picture: A data protection code of practice for surveillance cameras and personal information'* and the guidance published by the Information Commissioner's Office (ICO)- *'Video Surveillance Guidance'.*

31. Biometric Information (if relevant)

This type of information is considered as special category data. All such data must be handled appropriately and in accordance with *UK GDPR* and the *Data Protection Act 2018* principles.

Examples of biometric identification systems include fingerprinting and facial recognition systems (e.g., students using fingerprints to receive school dinners instead of paying with cash).

The school will obtain the written consent of pupils/parents/those with parental responsibility before recording and processing the pupil's biometric details. The consent form is available on the Data Protection page on the Learning Service Microsite.

Pupils/parents/those with parental responsibility can object to participation in the school's biometric recognition systems, or withdraw consent at any time, and the school will make sure that any relevant data already captured is deleted. Alternative methods of service provision must be identified if a parent/those with parental responsibility or pupil does not provide consent.

If the school is considering using live facial recognition technology (LFR), it must discuss this with the Schools Data Protection Officer before purchasing this technology. The school will need to demonstrate high standards of governance and accountability from the outset, including being able to justify that the use of LFR is fair, necessary, and proportionate in each specific context in which it is deployed. All risks will also need to be considered when using this new form of technology.

32. International Data Transfers

If intending on transferring any personal or special category data outside of the United Kingdom, this should be discussed with the Schools Data Protection Officer beforehand.

No personal or special category data may be transferred outside of the European Economic Area (EEA), which comprises the countries in the European Union and

Iceland, Liechtenstein, and Norway. This can be discussed further with the Schools Data Protection Officer if needed.

33. Business Continuity and Disaster Recovery

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.

The school has a Continuity Plan and a Disaster Recovery Plan in place in the event of incidents. These are also 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.

This includes identifying records that are critical to the continued functioning or reconstitution of school business. Also, where possible, a general description of the school's technical and organisational security measures is included in the school's *Records of Processing Activities (ROPA).*

The school will routinely back up data that is stored electronically to help restore information if needed.

The school will ensure that electronic records are protected during technological change e.g., during migration to new software or hardware platforms.

34. Training

The Headteacher and the Schools Data Protection Officer will ensure that staff are adequately trained regarding their data protection responsibilities. Headteachers, school governors and individuals whose roles require regular access to personal information, or who are responsible for implementing this policy, will receive additional training to help them understand their duties and how to comply with them.

All school staff will need to ensure that they have completed the mandatory *GDPR* and Cyber Awareness e-learning module training.

The Headteacher will keep a record of attendance and a central register of who has completed any data protection training and when they have completed it.

35. Breach of the Policy

Non-compliance with this policy by members of school staff could lead to serious consequences.

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

There is a risk of significant civil and criminal sanctions for the individual and the school authorities taken by third parties. An individual can commit a criminal offence under the *UK GDPR*, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the school.

Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could result in dismissal for gross misconduct.

If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

36. Review of Policy and Oversight Arrangements

This policy will be reviewed by the Schools Data Protection Officer on an annual basis. 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@anglesey.gov.wales

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/

Rhestr Termau, Diffiniadau a Deddfwriaeth Diogelu Data Ysgolion Dwyieithog

Schools Data Protection Bilingual Glossary, Definitions and Legislation

(Fersiwn 3, Hydref 2022 / *Version 3, October 2022*)

Geiriau a Termau / *Words and Terms*

Diffiniad	**Geiriau a Termau / *Words and Terms***	***Definition***
Casglu, meddiannu, cofnodi, trefnu, strwythuro, storio, dargadw, diwygio, addasu, altro, adennill, ymgynghori, lledaenu, cyfyngu, datgelu, dinistrio, dileu gwybodaeth neu ei defnyddio neu wneud unrhyw beth â hi.	**Prosesu gwybodaeth** ***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.*
Mathau o Wybodaeth / *Types of Information*		
Unrhyw wybodaeth ynglŷn ag unigolyn naturiol yr adnabyddir neu y gellir ei adnabod yn uniongyrchol neu'n anuniongyrchol drwy'r	**Data personol** ***Personal data***	Any information relating to an identified or identifiable natural person that can be identified either directly or indirectly from that

wybodaeth honno. Gellir ei storio'n ddigidol, ar gyfrifiadur, neu mewn systemau ffeilio ar bapur.		information. This can be stored electronically, on a computer, or in paper-based filing systems.
Gwybodaeth ynglŷn â hil, tarddiad ethnig, barn wleidyddol, credoau crefyddol neu athronyddol, aelodaeth undeb llafur (neu ddiffyg aelodaeth), gwybodaeth enetig, gwybodaeth fiometreg (i adnabod unigolyn) unigolyn, a gwybodaeth ynglŷn ag iechyd, bywyd rhywiol neu ogwydd rhywiol unigolyn. Data categori arbennig yw data personol sydd angen amddiffyniad bellach oherwydd ei fod yn sensitif.	**Data categori arbennig** ***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.*
Gwybodaeth bersonol yn ymwneud ag euogfarnau, troseddau, honiadau, achosion troseddol, a mesurau diogelwch cysylltiedig.	**Gwybodaeth am gofnodion troseddol** ***Criminal records information***	*Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.*
Data personol sy'n gysylltiedig ag iechyd corfforol neu feddyliol person naturiol, gan gynnwys darpariaeth gwasanaethau gofal iechyd, sy'n datgelu gwybodaeth am statws iechyd ef neu hi.	**Data ynghylch iechyd** ***Data concerning health***	*Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.*
Trydydd parti yw rhywun nad yw'n rheolwr data, yn brosesydd data nac yn wrthrych i'r data.	**Gwybodaeth Trydydd Parti** ***Third-party information***	*A third party is somebody who is not the data controller, the data processor, or the data subject.*
Data personol sy'n ymwneud â nodweddion genetig person a etifeddwyd neu a gaffaelwyd sy'n rhoi gwybodaeth unigryw am ffisioleg neu iechyd y person naturiol hwnnw ac sy'n deillio, yn benodol, o ddadansoddiad o sampl biolegol gan y person naturiol dan sylw.	**Data genetig** ***Genetic data***	*Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a*

		biological sample from the natural person in question.
Data personol sy'n deillio o brosesu technegol penodol sy'n ymwneud â nodweddion corfforol, ffisiolegol neu ymddygiadol person naturiol, sy'n caniatáu neu'n cadarnhau adnabyddiaeth unigryw'r person naturiol hwnnw, megis delweddau wyneb neu ddata dactyloscopig. Mae cydnabyddiaeth ôl bys yn enghraifft o ddata dactyloscopig.	**Data biometrig** ***Biometric data***	*Personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Fingerprint recognition is an example of dactyloscopic data.*
Mae technoleg adnabod wynebau byw (LFR), a elwir hefyd yn dechnoleg adnabod wynebau awtomatig, yn adnabod pobl mewn fideo mewn amser real, gan ddefnyddio set o ffotograffau fel cyfeiriad. Mae camerâu gwyliadwriaeth adnabod wynebau yn sganio'r holl wynebau y gallant eu gweld mewn torf i wirio hunaniaeth pobl yn erbyn cronfa ddata mewn amser real.	**Adnabod Wynebau Byw (LFR)** ***Live Facial Recognition (LFR)***	*Live facial recognition (LFR) technology, also known as automatic facial recognition, identifies people in a video in real time, using a set of photographs as a reference. Facial recognition surveillance cameras scan all the faces they can see in a crowd to check people's identity against a database in real-time.*
Rolau Diogelu Data / *Data Protection Roles*		
Y bobl neu'r sefydliadau sy'n pennu'r pwrpasau dros brosesu data personol, ac ym mha fodd y caiff ei brosesu. Mae gan y rheolydd data gyfrifoldeb i sefydlu ymarferion a pholisïau yn unol â deddfwriaeth. Yr ysgol yw'r rheolydd data.	**Rheolydd data** ***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.*
Yn cynnwys unrhyw berson sy'n prosesu data personol ar ran rheolydd data (heblaw am y sawl sy'n gyflogedig gan y rheolydd data). Gall proseswyr data gynnwys cyflenwyr sy'n ymdrin â data personol ar ran yr ysgol.	**Proseswyr data** ***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.
Unrhyw drydydd parti a benodir i brosesu data personol ar ran y prosesydd data.	**Is-brosesydd** ***Sub-processor***	*Any third party appointed to process personal data on behalf of the data processor.*
Yr unigolyn y mae'r wybodaeth bersonol yn ymwneud ag ef.	**Gwrthrych y data** ***Data subject***	*The individual to whom the personal information relates.*
Yn cynnwys gweithwyr sydd â'u gwaith yn ymwneud â data personol. Mae gan ddefnyddwyr data ddyletswydd i ddiogelu'r wybodaeth y maent yn ymdrin â hi drwy ddilyn polisïau diogelu data a diogelwch bob amser. Mae staff a gyflogir gan ysgolion yn ddefnyddwyr data.	**Defnyddwyr data** ***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.*
Mae DPO yn helpu i fonitro cydymffurfiaeth fewnol, hysbysu a chynghori ar rwymedigaethau diogelu data, rhoi cyngor ynghylch Asesiadau Effaith Diogelu Data (DPIAau) a gweithredu fel pwynt cyswllt ar gyfer gwrthrychau data a'r awdurdod goruchwylio.	**Swyddog Diogelu Data** ***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.*
Termau o yn berthnasol i brosesu data / *Terms relating to data processing*		
Mae sail gyfreithiol yn golygu, os yw sefydliad am brosesu data personol, fod angen nodi seiliau cyfreithiol penodol ar gyfer prosesu fel y'u diffinnir yn Erthygl 6 UK GDPR ac Erthygl 9 UK GDPR.	**Sail gyfreithiol** ***Legal basis***	*Legal basis means that if an organisation wants to process personal data, there is a need to identify specific legal grounds for the processing as defined in Article 6 UK GDPR and Article 9 UK GDPR.*
Gan y gwrthrych data yn golygu unrhyw arwydd rhydd, penodol, gwybodus a diamwys o ddymuniadau gwrthrych y data y mae ef neu hi, drwy ddatganiad neu drwy gam cadarnhaol clir, yn arwydd o gytundeb i brosesu data personol sy'n ymwneud ag ef neu hi. Mae'r baich o	**Caniatâd** ***Consent***	*Of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The burden of demonstrating*

ddangos caniatâd ar y rheolydd data.		*consent is on the data controller.*
Ystyr Cymalau Enghreifftiol yw'r cymalau cytundebol a gyhoeddwyd gan y Comisiwn Ewropeaidd i lunio trosglwyddiadau data gan Reolyddion a sefydlwyd yn yr EEA i Reolyddion a sefydlwyd y tu allan i'r EEA.	**Cymalau Enghreifftiol** ***Model Clauses***	*Model Clauses means the contractual clauses issued by the European Commission to frame data transfers from Controllers established in the EEA to Controllers established outside of the EEA.*
Termau yn berthnasol i Risg / *Terms relating to Risk*		
Effaith ansicrwydd ar amcanion. Risgiau i unigolion: y potensial am ddifrod neu drallod. Nodweddir risg yn aml gan gyfeirio at "ddigwyddiadau" a "chanlyniadau" posibl, neu gyfuniad o'r rhain.	**Risg** ***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.*
Adnabyddiad a dadansoddiad o risgiau i amcanion busnes y sefydliad.	**Asesiad Risg** ***Risk Assessment***	*The identification and analysis of risks to the organisation's business objectives.*
Beth fyddai canlyniadau'r risg pe bai'n digwydd. Effaith yn cael ei ystyried fel un sy'n cael effaith uniongyrchol neu effaith yn y dyfodol.	**Effaith** ***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.*
Pa mor debygol yw'r risg o ddigwydd – ansicrwydd, siawns a thebygolrwydd.	**Tebygolrwydd** ***Likelihood***	*How likely is it that the risk will occur- uncertainty, chance, and probability.*
Mesur sy'n addasu risg.	**Rheolaeth** ***Control***	*Measure that is modifying risk.*
Termau yn berthnasol i fesurau diogelwch / *Terms relating to security measures*		
Y broses lle prosesir gwybodaeth bersonol mewn ffordd na ellir ei defnyddio i adnabod unigolyn heb ddefnyddio gwybodaeth ychwanegol, a gadwir ar wahân ac yn amodol ar fesurau technegol a sefydliadol i sicrhau na ellir priodoli gwybodaeth bersonol i unigolyn a ellir ei adnabod.	**Ffugenwau** ***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.*

Cael gwared â gwybodaeth a ellir ei defnyddio i adnabod rhywun oddi ar rywbeth (megis data cyfrifiadur) fel na ellir gwybod beth oedd y ffynhonnell wreiddiol na'i hadnabod.	**Gwybodaeth Dienw** ***Anonymised***	*To remove identifying information from something (such as computer data) so that the original source cannot be known or identified.*
Mae amgryptio data yn ddull diogelwch lle mae gwybodaeth yn cael ei hamgodio a dim ond defnyddiwr sydd â'r allwedd amgryptio gywir y gall gael gafael ar neu ddadgryptio data. Mae data wedi'i amgryptio yn ymddangos wedi'i sgramblo neu'n annarllenadwy i berson neu endid sy'n cael mynediad heb ganiatâd.	**Amgryptio** ***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.*
Dilysu yw'r broses o benderfynu a yw rhywun (neu rywbeth) yn bwy (neu beth) y mae'n honni ei fod.	**Dilysu** ***Authentication***	*Authentication is the process of determining if someone (or something) is who (or what) it claims to be.*
Mae dilysu dau ffactor, wedi'i dalfyrio i 2FA, yn broses ddilysu sy'n gofyn am ddau ffactor dilysu gwahanol i sefydlu hunaniaeth - mae'n golygu ei gwneud yn ofynnol i ddefnyddiwr brofi ei hunaniaeth mewn dwy ffordd wahanol cyn rhoi mynediad iddynt i system.	**Dilysu ddau ffactor (2FA)** ***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.*
Termau yn berthnasol i ddiogelwch a digwyddiadau seibr / Terms relating to cyber security and incidents		
Cyfeiria seiberddiogelwch at y corff o dechnolegau, prosesau ac arferion sydd wedi'u cynllunio i ddiogelu rhwydweithiau, dyfeisiau, rhaglenni a data rhag ymosodiad, difrod neu fynediad heb awdurdod.	**Seiberddiogelwch** ***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.*
Mae ymosodiad seiber yn ymosodiad a gychwynnir o gyfrifiadur yn erbyn gwefan, system gyfrifiadurol neu gyfrifiadur unigol (gyda'i	**Ymosodiad Seiber** ***Cyber attack***	*A cyber-attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a*

gilydd, cyfrifiadur) sy'n peryglu cyfrinachedd, uniondeb neu argaeledd y cyfrifiadur neu'r wybodaeth a gedwir arno.		*computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.*
Mae haciwr yn unigolyn sy'n defnyddio cyfrifiadur, rhwydweithio neu sgiliau eraill i oresgyn problem dechnegol ac sy'n cael mynediad anghyfreithlon i wybodaeth mewn system gyfrifiadurol ac weithiau'n ymyrryd â hi.	**Hacwyr** ***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.*
Heb hawl cyfreithlon.	**Anawdurdodedig** ***Unauthorised***	*Without a legitimate right.*
Achos potensial o ddigwyddiad dieisiau, y gall arwain at niwed i system neu sefydliad.	**Bygythiad** ***Threat***	*Potential cause of an unwanted incident, which can result in harm to a system or organisation.*
Mae sgamwyr yn anfon e-byst ffug at filoedd o bobl yn gofyn am wybodaeth sensitif (fel manylion banc) neu'n cynnwys dolenni i wefannau drwg. Mae nhw'n gwneud hyn i ddwyn manylion er mwyn eu gwerthu neu o bosibl i gyrchu gwybodaeth sydd yn cael ei ddal gan sefydliadau.	**Gwe-rwydo** ***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.*
Meddalwedd sydd wedi'i gynllunio'n benodol i darfu, difrodi neu gael mynediad heb awdurdod i system gyfrifiadurol.	**Drwgwedd** ***Malware***	*Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.*
Term rhithwir ar gyfer mentro neu anfon negeseuon ymfflamychol mewn e-bost.	**Fflamio** ***Flaming***	*A virtual term for venting or sending inflammatory messages in an e-mail.*
Negeseuon amherthnasol neu ddigymell a anfonir dros y rhyngrwyd/e-bost, fel arfer at nifer fawr o ddefnyddwyr, at ddibenion hysbysebu, gwe-rwydo, lledaenu drwgwedd, ac ati.	**Sbam** ***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.*
Mae firws cyfrifiadurol yn fath o raglen gyfrifiadurol faleisus, sydd, pan gaiff ei gweithredu, yn ailadrodd ei hun ac yn	**Firws Cyfrifiadurol** ***Computer Virus***	*A computer virus is a kind of malicious computer program, which when executed, replicates itself*

mewnosod ei chod ei hun. Pan wneir yr atgynhyrchu, mae'r cod hwn yn heintio'r ffeiliau a'r rhaglenni arall sy'n bresennol ar y system.		*and inserts its own code. When the replication is done, this code infects the other files and program present on the system.*
Meddalwedd sy'n galluogi defnyddiwr i gael gwybodaeth gudd am weithgareddau cyfrifiadurol un arall drwy drosglwyddo data'n gudd o'u gyriant caled.	**Ysbïwedd** ***Spyware***	*Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.*
Rhaglen a gynlluniwyd i dorri diogelwch system gyfrifiadurol tra'n cyflawni rhywfaint o swyddogaeth ddiniwed.	**Trojan horses**	*A program designed to breach the security of a computer system while ostensibly performing some innocuous function.*
Unrhyw ddefnydd o gyfryngau cymdeithasol neu dechnoleg cyfathrebu i fwlio unigolyn neu grŵp.	**Bwlio seibr** ***Cyber bullying***	*Any use of social media or communication technology to bully an individual or group.*
Termau yn berthnasol i Technoleg Gwybodaeth / *Terms relating to Information Technology*		
Cyfrifiaduron prosesu gwybodaeth neu systemau cyfathrebu data.	**Systemau Gwybodaeth** ***Information Systems***	*Information processing computers or data communication systems.*
Mae storio cwmwl yn fodel cyfrifiadura cwmwl lle caiff data ei storio ar weinyddion o bell a gyrchir o'r rhyngrwyd, neu "gwmwl". Mae'n cael ei gynnal, ei weithredu a'i reoli gan ddarparwr gwasanaeth storio cwmwl ar weinyddion storio sy'n cael eu hadeiladu ar dechnegau rhithiol.	**Storio cwmwl** ***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.*
Mae'r gair "ap" yn dalfyriad ar gyfer *"application"* yn y Saesneg. Mae'n ddarn o feddalwedd sy'n gallu rhedeg drwy borwr gwe neu all-lein ar gyfrifiadur, ac ar ffôn clyfar, tabled neu ddyfeisiau electronig eraill.	**Ap** ***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.*
Mae system etifeddiaeth, a elwir hefyd yn blatfform etifeddiaeth (*legacy platform*),	**System Etifeddiaeth**	*A legacy system, also known as a legacy platform, is one that is based on*

yn un sy'n seiliedig ar dechnoleg neu offer sydd wedi darfod.	***Legacy System***	*obsolete technology or equipment.*
Unrhyw blatfform ar-lein sy'n cynnig rhyngweithio amser real rhwng y defnyddiwr ac unigolion neu grwpiau eraill. Mae enghreifftiau'n cynnwys, ond heb fod yn gyfyngedig i lwyfannau cyfathrebu, fforymau trafod ar-lein, blogiau, mannau cydweithredol, gwasanaethau rhannu cyfryngau, apiau micro-flogio a defnyddio gwe-gamerâu.	**Cyfryngau cymdeithasol** ***Social media***	*Any online platform that offers real-time interaction between the user and other individuals or groups. Examples include, but are not limited to communication platforms, online discussion forums, blogs, collaborative spaces, media sharing services, micro-blogging applications and the use of webcams.*
Mae dysgu cyfunol yn ddull cyfarwyddiadol sy'n cynnwys cyfuniad o weithgareddau dysgu ar-lein ac wyneb yn wyneb. Er enghraifft, gall myfyrwyr gwblhau aseiniadau hunan-gyflymder ar-lein erbyn dyddiad penodol ac yna cyfarfod ar y safle neu ar-lein ar gyfer gweithgareddau dysgu ychwanegol.	**Dysgu Cyfunol** ***Blended learning***	*Blended learning is an instructional approach that includes a combination of online and in-person learning activities. For example, students can complete online self-paced assignments by a certain date and then meet on-site or online for additional learning activities.*
Pan fydd dysgwyr yn cymryd rhan mewn cwrs dysgu ar-lein ar yr un pryd ond mewn gwahanol leoliadau, fe'i gelwir yn ddysgu cydamserol. Mae dysgu cydamserol yn caniatáu i ddysgwyr ryngweithio â'r hyfforddwr a chyfranogwyr eraill. Gwneir hyn drwy feddalwedd sy'n creu ystafell ddosbarth rithiol.	**Dysgu cydamserol (dysgu ar y pryd)** ***Synchronous learning (simultaneous learning)***	*When learners participate in an online learning course at the same time but in different locations, it is known as synchronous learning. Synchronous learning allows learners to interact with the instructor and other participants. This is done through software that creates a virtual classroom.*
Mae dysgu anghydamserol yn ddull o addysg lle mae disgyblion yn dysgu'r un cynnwys o wahanol leoedd (daearyddol) ac ar wahanol adegau. Gall disgyblion gael gafael ar ddeunyddiau, gofyn cwestiynau, ac ymarfer eu medrau ar unrhyw adeg sy'n gweithio iddyn nhw.	**Dysgu anghydamserol (dysgu nad yw'n ddysgu ar y pryd)** ***Asynchronous learning (non-simultaneous learning)***	*Asynchronous learning is an approach to education where pupils learn the same content from different (geographic) places and at different times. Pupils can access materials, ask questions, and practice their skills at any time that works for them.*

Mae'r ystafell ddosbarth rithiol yn cyfeirio at amgylchedd dysgu ystafell ddosbarth ddigidol sy'n digwydd dros y rhyngrwyd yn hytrach nag mewn ystafell ddosbarth ffisegol. Fe'i gweithredir drwy feddalwedd sy'n caniatáu i athro a myfyrwyr ryngweithio.	**Ystafell ddosbarth rithiol** ***Virtual classroom***	*The virtual classroom refers to a digital classroom learning environment that takes place over the internet rather than in a physical classroom. It is implemented through software that allows a teacher and students to interact.*
Mae cyfryngau ffrydio yn cyfeirio at fideo a sain sy'n cael ei lawrlwytho i gyfrifiadur o'r rhyngrwyd fel llif parhaus o ddata ac sy'n cael ei chwarae wrth iddo gyrraedd y cyfrifiadur cyrchfan.	**Cyfryngau ffrydio** ***Streaming media***	*Streaming media refers to video and audio that is downloaded to a computer from the internet as a continuous stream of data and is played as it reaches the destination computer.*
Gofodau ar y rhyngrwyd (safleoedd/tudalennau) lle gallwch gwrdd â phobl eraill a sgwrsio, naill ai mewn amser real (ystafelloedd sgwrsio a sgwrsio byw) neu drwy negeseuon a byrddau negeseuon.	**Gofod cymdeithasol ar-lein** ***Online social space***	*Internet areas (sites/pages) where you can meet other people and chat, either in real-time (chatrooms and live chat) or via messages and message boards.*
System wybodaeth ar y rhyngrwyd yw'r We Fyd-eang sy'n caniatáu i ddogfennau gael eu cysylltu â dogfennau eraill drwy ddolenni hyperdestun, gan alluogi'r defnyddiwr i chwilio am wybodaeth drwy symud o un ddogfen i'r llall.	**Gwe Fyd-eang (www.)** ***World Wide Web (www.)***	*World Wide Web is an information system on the internet which allows documents to be connected to other documents by hypertext links, enabling the user to search for information by moving from one document to another.*
Podlediad yw'r arfer o ddefnyddio'r rhyngrwyd i sicrhau bod recordiadau digidol o ddarllediadau ar gael i'w lawrlwytho i gyfrifiadur neu ddyfais symudol.	**Podledu** ***Podcasting***	*Podcasting is the practice of using the internet to make digital recordings of broadcasts available for downloading to a computer or mobile device.*
Tudalen we sy'n cynnwys ffenestr lle gallwch deipio testun i alluogi sgwrs 'amser real' ar ffurf testun gydag unigolion neu grwpiau bach.	**Ystafell sgwrsio** ***Chatroom***	*A web page that contains a window into which you can type text to enable a 'real-time' conversation in text form with individuals or small groups.*
Gwefan lle mae cofnodion rheolaidd yn cael eu gwneud ar ffurf cyfnodolyn neu	**Blog / Flog** ***Blog / Vlog***	*A website where regular entries are made in the form of an on-line journal or*

ddyddiadur ar-lein. Mae Blog neu 'log gwe' yn aml yn cynnig sylwebaeth neu newyddion ar bwnc penodol tra bod Flog yn defnyddio fideo i ddogfennu eu bywydau bob dydd fel dyddiadur fideo parhaus. Trefnir blogiau yn gronolegol fel arfer a chyda llai o ffurfioldeb na gwefan. Mae llawer o flogiau'n derbyn ac yn ymateb i sylwadau.		*diary. A Blog or 'web log' often offers commentary or news on a particular subject whilst Vlog uses video to document their daily lives as an ongoing video diary. Blogs are usually arranged chronologically and with less formality than a website. Many blogs accept and respond to comments.*
Gwefan neu adnodd tebyg sy'n caniatáu i ddefnyddwyr ychwanegu a golygu cynnwys gyda'i gilydd.	**Wici** ***Wiki***	*A website or similar resource that allows users to add and edit content collectively.*
Pecyn meddalwedd neu ap symudol am ddim yw porwr sy'n dangos tudalennau gwe, graffeg a'r rhan fwyaf o gynnwys ar-lein. Mae meddalwedd porwr wedi'i gynllunio'n benodol i drosi cod cyfrifiadurol HTML ac XML yn ddogfennau y gellir eu darllen gan bobl. Mae porwyr yn dangos tudalennau gwe.	**Porwr** ***Browser***	*A browser is a free software package or mobile app that displays web pages, graphics, and most online content. Browser software is specifically designed to convert HTML and XML computer code into human-readable documents. Browsers display web pages.*
Tudalen we yw'r hyn sydd i'w weld mewn porwr gwe pan fydd ar y rhyngrwyd. Gall tudalennau gynnwys testun, ffotograffau, delweddau, diagramau, dolenni, hysbysebion, a mwy ar unrhyw dudalen a welir.	**Tudalen We** ***Web Page***	*A web page is what can be seen in a web browser when on the internet. Pages may include text, photos, images, diagrams, links, advertisements, and more on any page that is viewed.*
URLau yw cyfeiriadau tudalennau a ffeiliau gwe ar borwr.	**URL**	*URLs are the web browser addresses of internet pages and files.*
Mae fideo-gynadledda yn delegyfathrebu ar ffurf fideo-gynhadledd sef cynnal cynhadledd ymysg pobl mewn lleoliadau anghysbell drwy gyfrwng signalau sain a fideo a drosglwyddir.	**Fideo-gynadledda** ***Videoconferencing***	*Videoconferencing is telecommunication in the form of a videoconference which is the holding of a conference among people at remote locations by means of transmitted audio and video signals.*

Mae PDA yn gyfrifiadur sy'n ffitio yng nghledr eich llaw i helpu i gasglu gwybodaeth fel cysylltiadau, apwyntiadau, ffeiliau a rhaglenni.	**Cymhorthion digidol personol (PDAau)** ***Personal digital aids (PDAs)***	*PDA is a computer that fits in the palm of your hand to help collect such information as contacts, appointments, files, and programs.*
Mae lawrlwytho yn derm eang sy'n disgrifio trosglwyddo rhywbeth ar y rhyngrwyd neu'r We Fyd-eang i gyfrifiadur neu ddyfais arall. Fel arfer, mae llwytho i lawr yn gysylltiedig â chaneuon, cerddoriaeth a ffeiliau meddalwedd.	**Lawrlwytho** ***Downloading***	*Downloading is a broad term that describes transferring something on the internet or the World Wide Web to a computer or another device. Commonly, downloading is associated with songs, music, and software files.*
System dechnegol yw Bluetooth sy'n caniatáu i bobl gyfnewid gwybodaeth a data gan ddefnyddio gwahanol fathau o ddyfeisiau electronig fel cyfrifiaduron, ffonau symudol, argraffwyr, camerâu fideo ac ati heb ddefnyddio gwifrau.	**Bluetooth**	*Bluetooth is a technical system that allows people to exchange information and data using different types of electronic devices such as computers, mobile phones, printers, video cameras, etc. without using wires.*
Termau yn berthnasol i E-byst / *Terms relating to E-mails*		
Negeseuon a ddosberthir drwy ddulliau electronig gan un defnyddiwr cyfrifiadur i un neu fwy o dderbynwyr drwy rwydwaith. Yn ogystal â chynnwys testunol, mae e-bost yn caniatáu i'r anfonwr anfon ffotograffau, fideo neu glipiau sain ar ffurf neu ffeiliau digidol.	**E-bost** ***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.*
Y gyrchfan y cyflwynir negeseuon post electronig iddi. Mae'n cyfateb i flwch llythyrau yn y system bost.	**Blwch Post** ***Mailbox***	*The destination to which electronic mail messages are delivered. It is the equivalent of a letter box in the postal system.*
Termau yn berthnasol i CCTV / *Terms relating to CCTV*		
Monitro symudiadau ac ymddygiad unigolion; gall hyn gynnwys fideo, sain neu ffilm fyw. At ddibenion y polisi hwn, dim ond fideos fydd yn berthnasol.	**Gwyliadwraeth** ***Surveillance***	*Monitoring the movements and behaviour of individuals; this can include video, audio, or live footage. For the purpose of this policy, only video footage will be applicable.*
Unrhyw ddefnydd o wyliadwriaeth nad yw ei	**Gwyliadwraeth Agored**	*Any use of surveillance for which authority does not fall*

hawdurdod yn dod o dan *Ddeddf Rheoleiddio Pwerau Ymchwilio 2000.*	***Overt surveillance***	*under the Regulation of Investigatory Powers Act 2000.*
Unrhyw ddefnydd o wyliadwriaeth nad yw'n cael ei rannu'n fwriadol â'r gwrthrychau y mae'n eu recordio. Ni fydd gwrthrychau'n cael gwybod am wyliadwriaeth o'r fath.	**Gwyliadwraeth cudd** ***Covert surveillance***	*Any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.*
Termau yn berthnasol i reoli cofnodion / *Terms relating to records management*		
Cadw'r wybodaeth yn gyflawn, yn gywir ac yn ddilys.	**Cywirdeb** ***Integrity***	*The preservation of the complete, accurate and validated state of information.*
Cofnodion sydd wedi'u dewis ar gyfer cadwraeth hirdymor oherwydd eu gwerth parhaus fel tystiolaeth neu fel ffynhonnell ar gyfer ymchwil hanesyddol neu ymchwil arall.	**Archifau** ***Archive***	*Records that have been selected for long term preservation because of their enduring value as evidence or as a source for historical or other research.*
Gellir adneuo cofnodion ar fenthyciad amhenodol ac os felly mae'r adneuwr yn cadw perchnogaeth ar y cofnodion. Mae gan yr adneuwyr yr hawl i dynnu eitemau'n ôl dros dro at ddibenion cyfreithiol, cyfeirio neu arddangosfa.	**Adneuo cofnodion** ***Depositing records***	*Records can be deposited on indefinite loan in which case the depositor retains ownership of the records. Depositors retain the right to temporarily withdraw items for legal purposes, reference, or exhibition.*

Termau a Dogfennau / *Terms and Documents*

Disgrifiad	**Termau a Dogfennau / *Terms and Documents***	***Description***
Mae'r Rhestr o Asedau Gwybodaeth yn cynnwys gwybodaeth am ba ddata a gedwir, lle caiff ei storio, sut y caiff ei ddefnyddio, pwy sy'n gyfrifol ac unrhyw reoliadau neu amserlenni cadw pellach a allai fod yn berthnasol.	**Rhestr o Asedau Gwybodaeth** ***Information Asset Register***	*The information asset register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.*

Mae angen i'r ROPA gynnwys yr holl ofynion perthnasol a nodir yn Erthygl 30 o'r UK GDPR. Mae'r ROPA yn rhestru pob gweithgaredd prosesu unigol; yn disgrifio union ddefnydd y data; y mesurau technegol a threfniadol sydd ar waith i ddiogelu'r data; pwy a effeithir gan y prosesu; dadansoddi risg a phroseswyr data posibl.	**Cofnodion o Weithgareddau Prosesu (ROPA)** ***Records of Processing Activities (ROPA)***	*The ROPA needs to contain all the relevant requirements set out in Article 30 of the UK GDPR. The ROPA lists every single processing activity; describes the exact usage of the data; the technical and organisational measures that are in place for the protection of the data; who is affected by the processing; risk analysis and possible data processors.*
Mae Hysbysiad Preifatrwydd yn rhoi gwybod i unigolion am yr wybodaeth bersonol sy'n cael ei chasglu ac sy'n cael ei chadw amdanynt a sut y gallent ddisgwyl i'w gwybodaeth bersonol gael ei defnyddio ac at ba ddibenion. Rhaid i'r Hysbysiad Preifatrwydd fod yn benodol i'r gweithgaredd sy'n gofyn am wybodaeth bersonol.	**Hysbysiad Preifatrwydd** ***Privacy Notice***	*A Privacy Notice informs individuals about the personal information that is collected and is held about them and how they can expect their personal information to be used and for what purposes. The Privacy Notice must be specific to the activity which requires personal information.*
Mae DPIA yn ofyniad cyfreithiol ar gyfer prosesu gweithgareddau sy'n debygol o fod yn risg uchel. Bydd DPIA yn cael ei wneud cyn dechrau'r prosesu, lle mae prosesu'n debygol o arwain at risg uchel i hawliau a rhyddid unigolyn (e.e., lle mae'r ysgol yn bwriadu defnyddio math newydd o dechnoleg).	**Asesiadau Effaith Diogelu Data (DPIAau)** ***Data Protection Impact Assessments (DPIA)***	*DPIAs are a legal requirement for processing activities that are likely to be high risk. A DPIA is performed before commencing the processing, where processing is likely to result in a high risk to an individual's rights and freedoms (e.g., where the school is planning to use a new form of technology).*
Mae cytundeb prosesu data yn gontract cyfreithiol rwymol sy'n nodi hawliau a rhwymedigaethau pob parti (rheolwr data a phrosesydd data) sy'n ymwneud â diogelu data personol. Mae angen cytundeb prosesu data ar y rheolwr data gydag unrhyw	**Cytundeb Prosesu Data (DPA)** ***Data Processing Agreement (DPA)***	*A data processing agreement is a legally binding contract that states the rights and obligations of each party (data controller and data processor) concerning the protection of personal data. The data controller needs a data processing agreement with*

bartïon sy'n gweithredu fel proseswyr data ar eu rhan.		*any parties that act as data processors on their behalf.*
Digwyddiad diogelwch sy'n arwain at ddinistrio, colli, addasu, datgelu'n anawdurdodedig neu fynediad at ddata personol a drosglwyddir, a storir neu a brosesir mewn unrhyw ddull arall gan yr ysgol, yn ddamweiniol neu'n anghyfreithlon.	**Digwyddiad Diogelwch Data** ***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.*
Lle datgelir data personol neu le ceir mynediad ato yn anawdurdodedig neu'n ddamweiniol.	**Digwyddiad cyfrinachedd** ***Confidentiality breach***	*Where there is an unauthorised or accidental disclosure of, or access to, personal data.*
Lle mae data personol yn cael ei newid yn anawdurdodedig neu'n ddamweiniol.	**Digwyddiad cywirdeb** ***Integrity breach***	*Where there is an unauthorised or accidental alteration of personal data.*
Lle mae colled mynediad at, neu ddinistr i ddata personol yn ddamweiniol neu'n anawdurdodedig.	**Digwyddiad argaeledd** ***Availability breach***	*Where there is an accidental or unauthorised loss of access to, or destruction of, personal data.*
Mae'r WASPI yn ffordd i sefydliadau sy'n ymwneud yn uniongyrchol ag iechyd, addysg, diogelwch, atal troseddu a lles cymdeithasol pobl yng Nghymru, rannu gwybodaeth bersonol yn effeithiol ac yn gyfreithlon.	**Cytundeb Rhannu Gwybodaeth Bersonol Cymru (WASPI)** ***Wales Accord on the Sharing of Personal Information (WASPI)***	*WASPI is a tool to help share personal information effectively and lawfully between organisations directly concerned with the health, education, safety, crime prevention and social well-being of people in Wales.*
Mae ISP yn cynorthwyo rhannu gwybodaeth bersonol yn rheolaidd a chyfartal rhwng rheolyddion data am reswm penodedig.	**Protocol Rhannu Gwybodaeth (ISP)** ***Information Sharing Protocol (ISP)***	*ISPs support, regular and reciprocal sharing of personal information between data controllers for a specified purpose.*
Mae DDA yn cynorthwyo datgelu gwybodaeth un ffordd o un rheolydd data i un neu fwy o reolyddion data am reswm penodedig.	**Gytundeb Datgelu Data (DDA)** ***Data Disclosure Agreement (DDA)***	*DDAs support one-way disclosures of information from a data controller to one or more data controllers.*
Dogfen sydd yn darparu digon o sicrwydd fod trydydd parti yn cydymffurfio â	**Tystysgrif Dinistr**	*A document that provides sufficient guarantees that a third party complies with*

chyfraith diogelu data pan yn dinistrio cofnodion ar ran yr ysgol.	***Certificate of Destruction***	*data protection law when disposing of records on behalf of the school.*
Mae Cais gan Wrthrych y Data (SAR) yn gais a wneir gan neu ar ran unigolyn am yr wybodaeth y mae ganddynt hawl i ofyn i sefydliad amdani o dan UK GDPR.	**Cais gan Wrthrych y Data** ***Data Subject Access Request***	*A Subject Access Request (SAR) is a request made by or on behalf of an individual for the information which they are entitled to ask an organisation for under the UK GDPR.*
Cais am wybodaeth a gedwir gan gyrff cyhoeddus o dan Ddeddf Rhyddid Gwybodaeth 2000.	**Cais Rhyddid Gwybodaeth (RhG)** ***Freedom of Information (FOI) Request***	*Request for information held by public bodies under the Freedom of Information Act 2000.*
Mae cyfrifoldeb rhiant yn golygu hawliau cyfreithiol, dyletswyddau, pwerau, cyfrifoldebau ac awdurdod sydd gan riant dros blentyn ac eiddo'r plentyn. Mae gan berson sydd â chyfrifoldeb rhiant dros blentyn yr hawl i wneud penderfyniadau am ei ofal a'i fagwraeth.	**Cyfrifoldeb Rhiant** ***Parental Responsibility***	*Parental responsibility means the legal rights, duties, powers, responsibilities, and authority a parent has for a child and the child's property. A person who has parental responsibility for a child has the right to make decisions about their care and upbringing.*
Y ffurflen SA3 ydi'r ffurflen swyddogol mae'r Heddlu yn gorfod ei defnyddio pan yn gwneud cais am wybodaeth personol.	**Ffurflen SA3- Cais i sefydliad allanol am ddatgelu data personol i'r Heddlu** ***SA3 Form- Request to external organisation for the disclosure of personal data to the Police***	*The SA3 form is the official form that the Police must use when making a request for personal information.*
Mae cytundeb lefel gwasanaeth yn gontract ffurfiol neu anffurfiol rhwng darparwr gwasanaeth mewnol neu allanol a defnyddiwr terfynol y gwasanaeth. Mae'n nodi'r hyn y bydd y cleient yn ei dderbyn ac yn egluro'r hyn a ddisgwylir gan y darparwr gwasanaeth.	**Cytundeb Lefel Gwasanaeth** ***Service Level Agreement***	*A service level agreement is a formal or informal contract between an internal or external service provider and the end user of the service. It specifies what the client will receive and clarifies what is expected of the service provider.*

Sefydliadau / *Organisations*

Disgrifiad	**Sefydliad / *Organisation***	***Description***
Yr ICO yw corff annibynnol y DU (awdurdod goruchwylio) a sefydlwyd i gynnal hawliau gwybodaeth. Rôl yr ICO yw cynnal hawliau gwybodaeth er budd y cyhoedd. Mae hyn yn cynnwys ymdrin â chwynion ynghylch problemau, cael gafael ar wybodaeth bersonol gan sefydliad, neu os oes pryderon ynghylch sut mae sefydliad wedi ymdrin â gwybodaeth - os yw'r wybodaeth yn anghywir, wedi'i cholli neu ei datgelu i rywun arall. Adroddir am achosion o dorri data sy'n risg uchel i unigolion i'r ICO. Ffôn: 0303 123 1113 Cyfeiriad: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Mae cyngor ac arweiniad ar gael drwy eu gwefan: www.ico.org.uk **Swyddfa ICO Cymru** Ffôn: 0330 414 6421 E-bost: wales@ico.org.uk Cyfeiriad: Swyddfa'r Comisiynydd Gwybodaeth – Cymru Yr Ail Lawr, Tŷ Churchill,	**Swyddfa'r Comisiynydd Gwybodaeth (ICO)** ***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.* *Telephone: 0303 123 1113* *Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF* *Advice and guidance are available via their website www.ico.org.uk* ***ICO Wales Office*** *Telephone: 0330 414 6421* *E-mail: wales@ico.org.uk* *Address: Information Commissioner's Office – Wales, 2nd Floor, Churchill House, Churchill Way, Cardiff, CF10 2HH*

Ffordd Churchill, Caerdydd, CF10 2HH		
Darparu ymateb effeithiol i ddigwyddiadau er mwyn lleihau niwed i'r DU, helpu gydag adferiad, a dysgu gwersi ar gyfer y dyfodol pan fydd digwyddiad seiberddiogelwch wedi digwydd- mae sefydliadau'n rhoi gwybod i'r NCSC am ddigwyddiadau seiber. Mae'r NCSC hefyd yn cydweithio â sefydliadau gorfodaeth ac amddiffyniad y gyfraith eraill, asiantaethau cudd-wybodaeth a diogelwch y DU a phartneriaid rhyngwladol. https://www.ncsc.gov.uk/	**The National Cyber Security Centre (NCSC)**	*Provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future when a cyber-security incident has occurred- organisations report cyber incidents to the NCSC.* *The NCSC also works collaboratively with other law enforcement, defence, the UK's intelligence and security agencies and international partners.* *https://www.ncsc.gov.uk/*
Mae gan yr Archifdy Cenedlaethol rôl o oruchwylio ac arwain ar gyfer y sector archifdy cyfan a'r proffesiwn archifdy yn y DU, gan gynnwys archifau llywodraeth leol ac anllywodraethol.	**Yr Archifdy Cenedlaethol** ***The National Archives***	*The National Archives has a role of oversight and leadership for the entire archives sector and archives profession in the UK, including local government and non-governmental archives.*

Deddfwriaeth, Deddfau a Chanllawiau / *Laws, Acts and Guidance*

Deddfwriaeth, Deddfau a Chanllawiau	***Laws, Acts and Guidance***
Rheoliad Diogelu Data Cyffredinol y Deyrnas Unedig (UK GDPR)	*The UK General Data Protection Regulation (UK GDPR)*
Deddf Diogelu Data 2018	*Data Protection Act 2018*
Cyfnodau Cadw Ysgolion 2018	*Schools Retention Period 2018*
Surveillance Camera Commissioner's Code of Practice- In the picture: A data protection code of practice for surveillance cameras and personal information	*Surveillance Camera Commissioner's Code of Practice- In the picture: A data protection code of practice for surveillance cameras and personal information*
Information Commissioner's Office (ICO) 'Subject access code of practice: Dealing with requests from individuals for personal information'	*Information Commissioner's Office (ICO) 'Subject access code of practice: Dealing with requests from individuals for personal information'*
Data Sharing Code of Practice	*Data Sharing Code of Practice*

Cod Plant - Dyluniad sy'n briodol i oedran: cod ymarfer ar gyfer gwasanaethau ar-lein.	*Children's Code- Age-appropriate design: a code of practice for online services*
Right of access: detailed guidance	*Right of access: detailed guidance*
Information Commissioner's Office (ICO)- Taking Photographs in Schools	*Information Commissioner's Office (ICO)- Taking Photographs in Schools*
Information Commissioner's Office (ICO) - 'Data controllers and data processors: what the difference is and what the governance implications are'.	*Information Commissioner's Office (ICO) - 'Data controllers and data processors: what the difference is and what the governance implications are'.*
The General Data Protection Regulation: Guidance on Consent (Information Governance Alliance)	*The General Data Protection Regulation: Guidance on Consent (Information Governance Alliance)*
Deddf Rhyddid Gwybodaeth 2000	*Freedom of Information Act 2000*
Deddf Hawliau Dynol 1998	*Human Rights Act 1998*
Protection of Freedoms Act 2012	*Protection of Freedoms Act 2012*
Rheoliadau Addysg (Gwybodaeth am Ddisgyblion) (Cymru) 2004	*The Education (Pupil Information) (Wales) Regulations 2004*
Llywodraeth Cymru - Deddf Gwasanaethau Cymdeithasol a Llesiant (Cymru) 2014, Gweithio Gyda'n Gilydd i Ddiogelu Pobl, Rhannu gwybodaeth i ddiogelu plant, Canllaw anstatudol i ymarferwyr, Gorffennaf 2019	*Welsh Government- Social Services and Well-being (Wales) Act 2014, Working Together to Safeguard People, Information sharing to safeguard children, Non-statutory guide for practitioners, July 2019*
Reoliadau Diogelu Data (Ffioedd a Gwybodaeth) 2018	*Data Protection (Charges and Information) Regulations 2018*
Information Commissioner's Opinion: The use of live facial recognition technology in public places	*Information Commissioner's Opinion: The use of live facial recognition technology in public places*