Data Protection Policy and Procedures

Schools handle increasing amounts of personal information and have a statutory requirement to comply with The Data Protection Act (DPA) which includes The General Data Protection Regulation (GDPR). Schools should have clear policies and procedures for dealing with personal information and be registered with the Information Commissioner's Office (ICO). Schools should have systems in place to reduce the chances of a loss of personal information, otherwise known as a data breach, which could occur as a result of theft, loss, accidental disclosure, equipment failure or hacking.

Aims & Objectives:

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived, and deleted/destroyed
- How staff, parents and pupils can access personal data

Ysgol Estyn is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, other schools and educational bodies, and potentially children's services. This policy is in place to ensure all staff and Governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (Wales) Regulations 2011
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

Data Protection Principles

The Data Protection Act establishes eight principles that must be adhered to at all times:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be adequate, relevant and not excessive
- Personal data shall be accurate and where necessary, kept up to date
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Personal data shall be kept secure i.e., protected by an appropriate degree of security
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of data protection

The GDPR also requires that the controller shall be responsible for, and able to demonstrate, compliance with the principles.

Data protection officer (DPO)

A DPO has been appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members
- The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools
- The DPO will report to the highest level of management at the school, which is the Headteacher
- The DPO will operate independently and will not be dismissed or penalised for performing their task
- Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations

Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. The DPA defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a Potential Data Breach, which could result in legal action against the school. The loss of sensitive personal data is considered much more seriously and the sanctions may well be more punitive.

Personal data

- The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:
- Personal information about members of the school community – including pupils / students, members of staff and parents / carers including names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular / academic data including class lists, pupil / student progress records, reports, references
- Professional records including employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Sensitive Personal data

- Sensitive personal data is defined by the Act as information that relates to the following 8 categories:
- race and ethnicity
- political opinions
- religious beliefs
- membership of trade unions
- physical or mental health
- sexual life
- criminal offences, criminal proceedings

Sensitive data requires a greater degree of protection and in a school it would include:

- Staff Trade Union details
- Information on the racial or ethnic origin of a child or member of staff
- Information about the sexuality of a child, his or her family or a member of staff
- Medical information about a child or member of staff
- Information relating to any criminal offence of a child, family member or member of staff

On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission should be sought from the parents / carers before posting information more widely.

Other types of Data not covered by the act

This is data that does not identify a living individual and therefore is not covered by the remit of the DPA but may fall under other access to information procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (If the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

Responsibilities

The Headteacher and Governing Body are responsible for Data Protection.

Risk Management - Roles
The school's Data Protection Assessor is the Head teacher. Their responsibilities are:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners **(IAOs**)

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the school. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process.

The school will identify Information Asset Owners (IAOs). In this school they are:

The school secretary and ICT co-ordinator

The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why

Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner
- Everyone in the school is expected to follow all processes and procedures in handling data
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor

Legal Requirements and lawful processing

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. The legal basis for processing data will be identified and documented prior to data being processed.

Lawful processing

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for:
    - Compliance with a legal obligation
    - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
    - For the performance of a contract with the data subject or to take steps to enter into a contract
    - Protecting the vital interests of a data subject or another person
    - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks)

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject

Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- 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 6 health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Information for Data Subjects (Parents, Staff)

To comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (e.g.LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through a letter – which may be sent in paper form or put on the school website.

Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes
- Where consent is given, a record will be kept documenting how and when consent was given
- The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR, however, acceptable consent obtained under the DPA will not be reobtained
- Consent can be withdrawn by the individual at any time
- The consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child

The right of access

- Individuals have the right to obtain confirmation that their data is being processed
- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data to verify the lawfulness of the processing
- The school will verify the identity of the person making the request before any information is supplied
- A copy of the information will be supplied to the individual free of charge; however, the school may impose a reasonable fee to comply with requests for further copies of the same information
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format
- Where a request is manifestly unfounded, excessive, or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information
- All requests will be responded to without delay and at the latest, within one month of receipt
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request
- Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal
- If a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to

The right to rectification

- Individuals are entitled to have any inaccurate or incomplete personal data rectified
- Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible
- Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to
- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex
- Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy

The right to erasure

- Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- Individuals have the right to erasure in the following circumstances:

    - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
    - When the individual withdraws their consent
    - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - The personal data was unlawfully processed
    - The personal data is required to be erased in order to comply with a legal obligation
    - The personal data is processed in relation to the offer of information society services to a child

- The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

    - To exercise the right of freedom of expression and information
    - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
    - For public health purposes in the public interest
    - For archiving purposes in the public interest, scientific research, historical research or statistical purposes
    - The exercise or defence of legal claims

- As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so
- Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question

The right to restrict processing

- Individuals have the right to block or suppress the school's processing of personal data
- If processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future
- The school will restrict the processing of personal data in the following circumstances:

    - Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
    - Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
    - Where processing is unlawful and the individual opposes erasure and requests restriction instead
    - Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
    - If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so
    - The school will inform individuals when a restriction on processing has been lifted

The right to data portability

- Individuals have the right to obtain and reuse their personal data for their own purposes across different service
- Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability
- The right to data portability only applies in the following cases:

    - To personal data that an individual has provided to a controller
    - Where the processing is based on the individual's consent or for the performance of a contract
    - When processing is carried out by automated means.

- Personal data will be provided in a structured, commonly used and machine-readable form
- The school will provide the information free of charge
- Where feasible, data will be transmitted directly to another organisation at the request of the individual
- The school is not required to adopt or maintain processing systems which are technically compatible with other organisations
- If the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual
- The school will respond to any requests for portability within one month
- Where the request is complex, or several requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request
- Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy

The right to object

- The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information
- Individuals have the right to object to the following:
    - Processing based on legitimate interests or the performance of a task in the public interest
    - Direct marketing
    - Processing for purposes of scientific or historical research and statistics
- Where personal data is processed for the performance of a legal task or legitimate interests
- An individual's grounds for objecting must relate to his or her particular situation
    - The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- Where personal data is processed for direct marketing purposes
    - The school will stop processing personal data for direct marketing purposes as soon as an objection is received
        - The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes
- Where personal data is processed for research purposes
    - The individual must have grounds relating to their particular situation in order to exercise their right to object
    - Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data
- Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online

Transporting, Storing and Deleting Personal Data

The policy and processes of the school will comply with the guidance issued by the ICO

Information security - Storage and Access to Data

Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation

- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e.owned by the users) must not be used for the storage of personal data
- The school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups

Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable not to record complete passwords, but prompts could be recorded.

Images

- Images of pupils will only be processed and transported by use of encrypted devices and permission for this will be obtained in the privacy agreement
- Images will be protected and stored in a secure area

Cloud Based Storage

- The school has clear policy and procedures for the use of Cloud Based Storage Systems and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data

Third Party data transfers

- As a Data Controller, the school is responsible for the security of any data passed to a third party. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

Retention of Data

- Government guidance will be used to determine how long data is retained
- Personal data that is no longer required will be destroyed and this process will be recorded

Systems to protect Data

Paper Based Systems

- All paper based official or official sensitive (or higher) material must be held in lockable storage, whether on or off site
- Paper based personal information sent to parents will be checked by a member of the senior management team before the envelope is sealed

School Websites

- Uploads to the school website will be checked prior to publication ensure that personal data will not be accidently disclosed and that images uploaded only show pupils where prior permission has been obtained

E-mail

- E-mails containing sensitive information should be encrypted, for example by attaching the sensitive information as a password protected word document. The recipient will then need to contact the school for access to a one-off password

Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information

- In the event of a data breach the DPO will inform the head teacher and chair of governors
- The term personal data breach refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
- The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed
- All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it
- The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case by-case basis
- If a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly
- A high risk breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority
- If a breach is sufficiently serious, the public will be notified without undue delay
- Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified
- Within a breach notification, the following information will be outlined:

    - The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
    - The name and contact details of the DPO
    - An explanation of the likely consequences of the personal data breach
    - A description of the proposed measures to be taken to deal with the personal data breach
    - Where appropriate, a description of the measures taken to mitigate any possible adverse effects

- Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself

A summary of Data Security measures and procedures

- Confidential paper records are kept compliantly and destroyed ASAP
- Confidential paper records are not be left unattended or in clear view anywhere with general access
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet or storage wall, drawer or safe when not in use
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted
- All electronic devices are password-protected to protect the information on the device in case of theft
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft
- Staff and governors do not use their personal laptops or computers for school purposes unless they are personally password-protected and fully encrypted
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data
- Before sharing data, all staff members ensure:

    - They are allowed to share it
    - That adequate security is in place to protect it
    - Who will receive the data has been outlined in a privacy notice

- Under no circumstances are visitors allowed access to confidential or personal information Visitors to areas of the school containing sensitive information are supervised at all times
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place
- Our school takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action
- The school business manager/Office manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data
- Pupils assessment information is held on Assessment Manager. This is password protected and encrypted and only accessible to relevant staff
- Pupil data is held within SIMS. SIMS access is password protected and passwords are only distributed to relevant staff
- The school utilises a strong system of firewalls to deter any internet attack
- All staff emails are password protected
- All devices that can access pupil, staff details are password protected

Policy Review Reviewing

This policy will be reviewed and updated every year.