Ysgol Gyfun Gymraeg Llangynwyd

Data Protection Policy

Data Protection Policy

Introduction

Ysgol Gyfun gymraeg Llangywnyd collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to inform individuals including parents and pupils of the information that it holds. This information should summarise why it is held and any other parties to whom this may be passed on to. Schools will advise individuals through Fair Processing in concise, transparent, plain language and free of charge.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation (GDPR), and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data that relates to a living individual who can be identified from that data, or other information held as defined within the GDPR.

General Data Protection Regulation (GDPR) Principles:

The GDPR establishes six enforceable principles that must be adhered to at all times in that information must be:

1. Processed fairly, lawfully and in a transparent manner
2. Collected for specified explicit and legitimate purposes and not further processed in a manner that is incompatible for those purposes.
3. Adequate relevant and limited to what is necessary in relation to the purpose for which it is processed
4. Accurate and where necessary kept up to date
5. Kept in a form that permits identification of data subjects for no longer than necessary for purposes that which the personal data is processed
6. Processed in a manner that ensures appropriate security of the personal data

General Statement

The school is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as right of access, right of rectification, right to erasure, right to restrict processing, right to data portability and right to object
- Ensure our staff are aware of and understand our policies and procedures
- Ensure our staff are provided with adequate training and support

Rights of access to information

There are two distinct rights of access to information held by schools about pupils:

1. Under the GDPR any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

Individual Rights

The GDPR provides the following rights for individuals:

1. **The right to be informed**

The school will provide concise, transparent, intelligible and easily accessible information about the processing of personal data to individuals via the Privacy Notice. This will be written in clear plain language and will clearly set out how personal data is processed within the school.

2. **The right of access**

The school will provide individuals with access to their personal data and supplementary information; this will be processed as a subject access request. Subject Access Requests will be free of charge and processed in line with the statutory requirements and timeframes.

3. **The right to rectification**

The school is committed to rectifying personal data if inaccurate or incomplete and notifying any relevant third parties of this.

The school will respond to a request for rectification within one month of receiving the request, if the request for rectification is deemed complex this will be responded to within two months.

If the school cannot take action in response to a request for rectification we will provide a written explanation of this, an individual will then have a right to complain to the school's data protection officer.

4. **The right to erasure**

The school will consider individual requests for deletion or removal of personal data where there is no compelling reason for its continued processing.

Schools will inform relevant third parties of erasure of personal data; unless it is impossible, involves disproportionate effort to do so.

5. **The right to restrict processing**

The school will ensure that data processing is restricted in any of the following circumstances:

- Where an individual's contests the accuracy of personal data until the accuracy is verified
- Where an individual has objected to the processing
- When processing is unlawful
- If the school no longer requires to keep the personal data but the induvial requires the data in relation to a legal claim

If data processing is restricted, the school will notify any relevant third parties.

6. **The right to data portability**

The school will comply with individual requests to data portability free of charge and within one month of receiving the request.

7. **The right to object**

The school will comply with individuals right to object and will stop processing personal data unless there are compelling legitimate grounds for processing or the processing is in relation to a legal claim.

The school will inform individuals of their right to object at the point of first communication in the schools Privacy Notice.

8. Rights in relation to automated decision making and profiling

The school will not use automated decision making nor profile any individuals.

The school clearly sets out within its Privacy Notice what information we collect/use and why this is relevant.

Subject Access Requests

The school will process all subject access requests and provide a copy of the information free of charge and within one month of receipt.

The school will charge a fee when a request is manifestly unfounded or excessive, particularly if it is repetitive,

Further copies of the information can be provided at a reasonable charge,

If requests are complex or numerous the school has the right to extend the period of compliance by a further two months. The school will notify individuals if this occurs.

If a request is manifestly unfounded or excessive the school has the right to refuse this request, the school will notify the individual and explain why they cannot comply with the request and inform them of their right to complain to the school's data protection officer.

The school will verify the identity of the individual making the request using reasonable means. For further information about Subject Access Requests, see Appendix 1 of this policy.

Complaints

Complaints in relation to processing of personal data should be addressed to the school's data protection officer.

Data Protection Officer (DPO)

Please find below details of the School's Data Protection Officer: -
Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the school to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed;

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach;

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Review

This policy will be reviewed on an annual basis. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Mr. Meurig Jones (Headteacher) on 01656 815700 who will also act as the contact point for any requests for personal data.

Further advice and information are available from the Information Commissioner's Office:

www.ico.org.uk

The Information Commissioner's Office - Wales
2nd Floor – Churchill House

Churchill Way

Cardiff

CF10 2HH

Telephone: **0330 414 6421** – Helpline is open from 9am to 5pm, Monday to Friday

Email: wales@ico.org.uk

Signed (Chair of Governors) _____

Date_____

Signed (Headteacher) _____

Date_____

Appendix 1 – Subject Access Requests

Under Data Protection Law, Data Subjects have a general right to find out whether the school hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the school are undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled, and for all individuals on how to make a SAR. Failure to comply with the right of access under UK GDPR puts both staff and the school at potentially significant risk, and so the School takes compliance with this policy very seriously.

A Data Subject has the right to be informed by the school of the following: -

(a) Confirmation that their data is being processed;
(b) Access to their personal data;
(c) A description of the information that is being processed;
(d) The purpose for which the information is being processed;
(e) The recipients/class of recipients to whom that information is or may be disclosed;
(f) Details of the school's sources of information obtained;
(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
(h) Other supplementary information.

How to recognise a subject access request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the school process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g. during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the school hold about me' will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

How to make a data subject access request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the school to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

What to do when you receive a data subject access request

All data subject access requests should be immediately directed to the Headteacher] who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the school must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual without delay and failure to do so may result in disciplinary action taken.

Acknowledging the request

When receiving a SAR the school shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the school may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the school must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The school should work with their DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a SAR, the school will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The school is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the school has reasonable doubts as to the identity of the individual making the request, evidence of identity may be

established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement. If an individual is requesting a large amount of data the school may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The school shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the school do not receive this information, they will be unable to comply with the request.

Requests made by third parties or on behalf of children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The school may also require proof of identity in certain circumstances.

If the school is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the school should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the school is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the school will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The school may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

Fee for responding to a SAR

The school will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the school will inform the requester why this is considered to be the case and that the school will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The school has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the school is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third-party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the school will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School closure periods

Requests received during or just before school closure periods may not be able to be responded to within the one calendar month response period. This is because we do not review emails during this period.

As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e. until a time when we receive the request), however, if we can acknowledge the request we may still not be able to deal with it until the school re-opens. The school will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Company rectifies, erases or restricts the processing of his personal data; or
    - to object to its processing;
    - to lodge a complaint with the ICO;
    - where the personal data has not been collected from the individual, any information available regarding the source of the data;
    - any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly-used electronic format.

The information that the school are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the school have one month in which to respond the school is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The school is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The school is not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data the school need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the school may need to search all or some of the following:

- electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The school should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Protection of third parties -exemptions to the right of subject access

There are circumstances where information can be withheld pursuant to a SAR.

These specific exemptions and requests should be considered on a case by case basis.

The school will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the school do not have to disclose personal data to the extent that doing so would

involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individuals consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances the school may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The school do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The school do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the school receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the school must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The school do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The school do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The school do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to respond to a request

The school can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the school can:

- request a “reasonable fee” to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

Record keeping

A record of all subject access requests shall be kept by the Data Protection Officer. The record shall include the date the SAR was received, the name of the requester, what data the school sent to the requester and the date of the response.

Appendix 2 – Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of identity: We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e. the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information *If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.*
Details:

Employment records: If you are, or have been employed by the school and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc. **Details:**

Section 2
Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	

Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

What is your relationship to the data subject? (e.g. parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g. time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to:
post@ygglangynwyd.pen-y-bont.cymru

Appendix 3 – Data Breach Policy

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the school of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the school's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

What Is A Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

When Does It Need To Be Reported?

The school must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;

- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

Reporting A Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should report to the Headteacher or the Data Protection Officer.

Where appropriate, you should liaise with your line manager about completion of the data report. Breach reporting is encouraged throughout the school and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, the Headteacher or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The school will acknowledge receipt of the data breach report and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording The Breach

On being notified of a suspected personal data breach, the school will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the school's data breach register;
- Notify the ICO where required;
- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

Notifying the ICO

The DPO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If the school are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the school will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the school have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the school will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the school will consider alternative means to make those affected aware (for example by making a statement on the school website).

Notifying Other Authorities

The school will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

Assessing The Breach

Once initial reporting procedures have been carried out, the school will carry out all necessary investigations into the breach.

The school will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the school will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the school will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the Headteacher or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

Training

The school will ensure that staff are trained and aware on the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them. This policy will be shared with staff.