Tasker Milward VC School – Strive to Achieve Respect

Ysgol RG Tasker Milward- Safwn Er mwyn Rhagoriaeth

Data Protection Policy

Issue No Rhif y Cyhoeddiad	Author / Owner Awdur/ Perchennog	Date Written Dyddiad Ygrifennwyd	Approval by Governors on Cymeradwywyd gan y llywordraethwyr	Comments Sylwadau
2	HT	June 2012	November 2012	Update
3	MT-J	January 2016	March 2016	

DATA PROTECTION POLICY

Tasker Milward VC School 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 be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice (Appendix 2) to all pupils/parents; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose
This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, 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 which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles
The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. 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.

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 Subject Access Requests (Appendix 1).
- Ensure our staff are aware of and understand our policies and procedures

Information Security Breach
In the event of a security breach the procedures detailed in appendix 3 will be followed.

Complaints
Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Privacy Impact Assessments
Privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of a project or existing procedures. When undertaking a Privacy Impact Assessment the school follows the published Information Commissioner's Office Code of Practice.

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. 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 Mrs H Lewis, Headteacher, who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745 3

Appendix 1

Tasker Milward VC School
Procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information
There are two distinct rights of access to information held by schools about pupils.
1. Under the Data Protection Act 1998 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.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request
1. Requests for information must be made in writing; which includes email, and be addressed to Mrs H Lewis, Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.
3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to
consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.
4. The school may make a charge for the provision of information, dependant upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 40 days will not commence until after receipt of fees or clarification of information sought
6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.
7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school.
Before disclosing third party information consent should normally be obtained.
There is still a need to adhere to the 40 day statutory timescale.
8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
9. If there are concerns over the disclosure of information then additional advice should be sought.
10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.
The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints
Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.
Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts
If you have any queries or concerns regarding these policies / procedures then please contact Mrs H Lewis, Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

Appendix 2

Ysgol Tasker Milward
Fair Processing Notice - Data Protection Act 1998

This leaflet tells you about what the **Welsh Government**, **Pembrokeshire Education Services** and **Tasker Milward VC School** does with your child's, personal and performance information (data), and any personal information (data) relating to you as parent / guardian.

The Collection of Personal Information

The school collects information about pupils and their parents or legal guardians when they go to a new school, they also collect information at other times during the school year. Information is also received from other schools when pupils transfer. The Local Authority (LA) and Welsh Government (WG) will receive information on pupils / students from the school / educational establishment, normally as part of what is called the Pupil Level Annual Schools Census which takes place in January each year. The school, LA and Welsh Government receive information about exam and national curriculum assessment and test results.

Personal information held

The sort of personal information that will be held includes;

- personal details such as name, address, date of birth, contact details for parents and guardians and also pupils photographs;
- information on performance in internal and national assessments and examinations;
- information on the ethnic origin and national identity of pupils (this is used only to prepare summary statistical analyses);
- details about pupils' immigration status (this is used only to prepare summary statistical analyses);
- medical information needed to keep pupils safe while in the care of the school;
- information on attendance and any disciplinary action taken;
- information about the involvement of social services with individual pupils where this is needed for the care of the pupil.

Other information

The WG, LA and school will try to ensure that information is accurate and secure. Personal information will not be sent outside the United Kingdom.

The use made of this personal information

The WG uses the information collected to do research, primarily to inform educational policy changes and funding. The research is done in a way that ensures individual pupils cannot be identified. Examples of the sort of statistics produced can be viewed at www.learning.wales.gov.uk or www.wales.gov.uk/statistics The LA also uses the personal information collected to do research. It uses the results of the research to make decisions on policy and the funding of schools, to calculate the performance of schools and help them to set targets. The School may use personal information to contact parents and

guardians by mobile phone or email. The School and LA also uses the information it collects to administer the education it provides to pupils. For example;

- the provision of educational services to individuals;
- monitoring and reporting on pupils' / students' educational progress;
- the provision of welfare, pastoral care, and health services; SEN and transport requirements;
- exclusions and attendance data
- the giving of support and guidance to pupils / students, their parents and legal guardians;
- the organisation of educational events and trips;
- planning and management of the school.
- recording of monetary payments to and from pupils and parents/carers.

Organisations who may share personal information

Information held by the School, LA and the WG on pupils, their parents or carers may be shared with other organisations when the law allows, for example with;

- other education and training bodies, including schools, when pupils are applying for courses, training, school transfer or seeking guidance on opportunities;
- bodies doing research for the WG, LA and schools, so long as steps are taken to keep the information secure;
- central and local government for the planning and provision of educational services;
- social services and other health and welfare organisations where there is a need to share information to protect and support individual pupils;
- various regulatory bodies, such as ombudsmen, inspection authorities and Government fraud initiatives, where the law requires that information be passed on so that they can do their work.

Regional Education Services

The school and the Local Authority will share information with regional education services for the purposes and benefit of:

- Maintaining accurate data.
- Delivery of education services – regional and local.
- Provision of statutory, Consortium and Authority returns.
- Analysing and reporting performance of pupils, schools, services, Authorities and the Consortium.

Data will be held and shared in an appropriate and secure manner.

Your rights under the Data Protection Act 1998

The Data Protection Act 1998 gives individuals certain rights in respect of personal information held on them by any organisation. These rights include;

- the right to ask for and receive copies of the personal information held, although some information can sometimes be legitimately withheld;
- the right, in some circumstances, to prevent the processing of personal information if doing so will cause damage or distress;
- the right to ask for wrong information to be put right;
- the right to seek compensation for damages caused by a breach of the Act.

- in some circumstances a pupil's parent or legal guardian may have a right to receive a copy of personal data held about a pupil in their legal care. Such cases will be considered on an individual basis where the individual is deemed to have insufficient understanding of their rights under the Act.

You also have the right to ask the Information Commissioner, who enforces and oversees the Data Protection Act 1998, to assess whether or not the processing of personal information is likely to comply with the provisions of the Act.

Seeking further information

For further information about the personal information collected and it's use, if you have concerns about the accuracy of personal information, or wish to exercise your rights under the Data Protection Act 1998, you should contact;

- Tasker Milward VC School on **01437 764147**
- Pembrokeshire County Council on **01437 764551**
- the Welsh Government data protection officer at, Welsh Government, Cathays Park, Cardiff, CF10 3NQ;
- the Information Commissioner's office help line can be contacted on 01625 545 745;
- information is also available from www.informationcommissioner.gov.uk

Appendix 3

Security Breach Procedures

All security breaches are reported to the Headteacher. The Headteacher may then appoint another member of the management team to investigate the breach and record the details.

Recording of details should be accurate, using the form at the end of these procedures.

Details of serious security incidents can be very sensitive and any sensitive information must be handled with discretion and only disclosed to those who need to know the details.

Staff must not attempt to conduct their own investigations, unless authorised to do so, to ensure evidence is not destroyed.

Any decision to take disciplinary action will be in line with the School's Disciplinary Policy.

.

Data Breach Management Plan - Responsibility of Information Governance
Breach Management Plan

The Headteacher (or nominated person) will lead all data breach investigations and will follow the Information Commissioner's Office (ICO) suggested Breach Management Plan: -

1. Containment and recovery.
2. Assessment of ongoing risk.
3. Notification of breach.
4. Evaluation and response.

1. Containment and Recovery

Containment and recovery involves limiting the scope and impact of the data breach, and stemming it as quickly as possible.

Where there is a risk that illegal activity might occur in the future the Headteacher and investigating Officer must consider whether the police need to be informed. An example of illegal activity is theft.

The Headtecher or nominated person will lead an investigation.

The investigating Officer wil quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occuring, recover any losses and limit the damage. Steps **might** include: -

- Attempting to recover any lost equipment or personal information.
- Shutting down an IT system.
- Inform staff so that they are prepared for any potentially inappropriate enquiries about the affected data subjects. If an inappropriate enquiry is received staff should attempt to obtain the enquirer's name/contact details and confirm that they will ring the enquirer back.
- Contacting the County Council Press Office so they can be prepared to handle any press enquiries or to make any press releases.

- The use of back-ups to restore lost, damaged or stolen information.
- If bank details have been lost/stolen consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant staff informed.

2. Assessment of Ongoing Risk / Investigation

The next stage of the management plan is for the Investigating officer to investigate the breach and assess the risks arising from it.

The Investigation Officer should ascertain whose information was involved in the breach, the potential effect on the data subjects and what further steps are required to remedy the situation.

The investigation should consider: -

- The type of information.
- Its sensitivity.
- How many individuals are affected by the breach?
- What protections are in place (e.g. encryption)?
- What happened to the information?
- Whether the information could be put to any illegal or inappropriate use.
- What could the information tell a third party about the individual?
- How many people are affected?
- What types of people have been affected (the public, supplier, staff, etc)?
- Whether there are wider consequences to the breach?

The investigating officer should keep a clear report detailing the nature of the breach, steps to preserve evidence, the assessment of risk/investigation, and the actions taken to mitigate the breach, any notifications made and recommendations for future work/actions.

The initial investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved

3. Notification

The Headteacher, after seeking legal advice and working with the Investigating Officer should decide whether anyone, such as the Information Commissioner's Office (ICO) or the data subjects, should be notified of the breach. The headteacher will make any notifications to the ICO. The headteacher and the investigating officer will decide whether and how anybody else should be notified.

Every incident will be considered on a case-by-case basis but if the breach is significant and involves personal information the ICO should be notified. There is guidance on the ICO website about how and when to notify - www.ico.gov.uk. The following points will be used to assist in deciding whether to notify an organisation such as the ICO or the data subjects: -

- Do we have any legal/contractual obligations in relation to notification?
- Would notification help prevent the unauthorised or unlawful use of the personal information?

- Could notification make the unauthorised or unlawful use of the personal information more likely?
- Could notification help the data subject – could they act on the information to mitigate risks?
- If the information is personal or sensitive personal in nature and there are large numbers of data subjects involved or possible serious consequences we should notify the ICO.
- The dangers of over notifying, which may cause disproportionate enquiries and work.

Notifications should include a description of how and when the breach occurred, what information was involved and what has already been done to mitigate the risks.

When notifying data subjects, specific and clear advice should be given on what individuals can do to protect themselves and what the council can do to assist them.

Details should be provided of how to make a complaint to the council and how to appeal to the Information Commissioner.

4. Review and Evaluation

Once the initial after effects of the breach are over Headteacher should fully review both the causes of the breach and the effectiveness of the response to it, and determine if any further control improvements are required.

The headteacher will inform the Governors of the breach and the action taken.

If issues are identified an action plan must be drawn up to put these right.