



Maendy Primary School

Personal Data Handling Policy

Date of this review: December 2015

Date of next review: Autumn 2016

Signed:

Date: Chair of Governors

Introduction

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

It is a statutory requirement for all schools to have a Data Protection Policy: Recent publicity about data breaches suffered by organisations and individuals has made the area of personal data protection compliance a current and high profile issue for schools and other organisations. Maendy Primary School has a personal data handling policy in order to avoid / minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure.

In addition:

- No individual would want to be the cause of any data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Schools are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The school will want to avoid the criticism and negative publicity that could be generated by any personal data breach.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

Maendy Primary School and all its employees will do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The DPA (Data Protection Act) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines "Personal Data" as data which relate to a living individual who can be identified:

- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Personal Data

The school and individuals 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, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" (See section below) and lawfully processed in accordance with the "Conditions for Processing".

Responsibilities

The school's Data Protection Officer and Senior Information Risk Officer (SIRO) is Mrs. J Cresswell. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risks and risk assessments
- appoint Information Asset Owners (IAOs)

The school has designated Information Asset Owners (IAOs): Mrs Bellew / Mrs Baker / Miss Prosser, for the various types of data being held (e.g. pupil information / staff information / assessment data etc). 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, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

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.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Data Protection Register - Entry Details

Registration Number: Z8048846

Date Registered: 10 October 2003 Registration Expires: 09 October 2017
description of processing

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

Reasons/purposes for processing information

We process personal information to enable us to:

- provide education, training, welfare and educational support services
- administer school property
- maintain our own accounts and records
- carry out fundraising
- support and manage our employees

We also use CCTV systems to monitor and collect visual images for security and the prevention of crime.

Type/classes of information processed

We process information relating to the above reasons/purposes. This information may include:

- name and personal details
- family, lifestyle and social circumstances
- financial details
- education details

- employment details
- student and disciplinary records
- vetting checks
- goods and services
- visual images, personal appearance and behaviour

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- trade union membership
- sexual life
- offences and alleged offences

Who the information is processed about

We process personal information about:

- our students and pupils
- advisers and other professional experts
- school staff
- members of school boards
- donors and potential donors
- suppliers
- complainants and enquirers
- individuals captured by CCTV images

Who the information may be shared with

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- education, training, careers and examining bodies
- school staff and boards
- family, associates and representatives of the person whose personal data we are processing
- local and central government
- healthcare professionals
- social and welfare organisations
- police forces
- courts
- current, past or prospective employers
- voluntary and charitable organisations
- business associates and other professional advisers
- suppliers and service providers
- financial organisations
- security organisations
- press and the media

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the data protection act.

Information to Parents / Carers – the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, Maendy Primary School will inform parents / carers of all pupils of the data we collect, process and hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, WG, etc) to whom it may be passed, through the use of a “Privacy Notice” (See Appendices).

This privacy notice will be passed to parents / carers through the annual report to parents from Governors, and is published on the school's website.

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

All staff are aware of the need to use secure school email systems when dealing with potentially sensitive personal information.

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Secure Storage of and access to data

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.

All users will use strong passwords which must be changed regularly. User passwords must never be shared. (See password policy section of E-safety & Acceptable Use Policy for further detail).

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).

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. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

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 device must offer approved virus and malware checking software, and
- the data must be securely deleted from the device, in line with the Staff Acceptable Use of ICT Policy once it has been transferred or its use is complete.

The authority has clear procedures for the automatic backing up, accessing and restoring of data held on school systems.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (See Cloud-based storage section of E-Safety & Acceptable Use Policy) 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.

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.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under

certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location;
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school;
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log is kept of all electronic equipment that is disposed of in compliance with the WEEE (Waste Electrical and Electronic Directive) recycling scheme. The log includes the asset numbers, classification, date of destruction, method and authorisation.

Appendices:

Additional issues related to Personal Data Handling:

Use of Cloud Services

Just as a school has obligations around data on its physical network, the same obligations are required when dealing with data in the cloud i.e. it is still required to be protected in line with the Data Protection Act (DPA) and may be subject to Freedom of Information (FOI) requests.

Freedom of Information

FOI may require anything written in an official capacity to be potentially made public. This might mean you need to consider how long content is stored for and the ease of which it can be recovered from a cloud archive. Cloud services very often are not designed for the long-term storage of content, particularly transient communications with high volume like email. Schools should consider how to secure and back-up to a local system what could be sensitive or important data.

Safeguarding

There are also safeguarding obligations for the use of technology at Maendy (in partnership with Torfaen SRS) which include:

- Effectively monitoring the use of systems to detect potential and actual safeguarding issues
- Monitoring, alerting and responding to illegal activity
- Providing consistent safeguarding provision both within and beyond school if devices/services leave the site

Criminal Activity

Maendy Primary School has an immediate obligation to report illegal or criminal activity to the Police.

Where is the cloud?

Most education systems have to make use of personal information to function. The DPA (Principle 8) states that personal data must not be transferred to any other country without adequate protection in situ. Data protection requirements vary widely across the globe. Countries in the EU approach privacy protection differently to those outside and are more stringent in the detail and responsibilities of data users than perhaps the US. Microsoft Office 365 is held in data centres in Amsterdam and Dublin.

Security concerns

Data centres are required to have stringent physical interventions in place against data being compromised from internal or external access. There are sophisticated security mechanisms in place to prevent external hacking of data. Whilst this cannot always be guaranteed to be 100% safe, this sophistication is often beyond the local capability of a single school and so can be regarded as reasonable duty of care.

Access to data through devices is much more likely given that devices are going to and from school in bags, on buses, or left lying around at home or school. If a device goes missing or breaks, the big advantage of cloud systems is that, apart from simple local settings, content is in the cloud so data is not 'lost' in the same way as if a laptop is stolen or suffers a hard drive failure. Cloud services can offer device management systems that can lock or locate a device if missing.

Passwords and authentication are critical at any point in securing access to data but are especially so with data in the cloud.

At Maendy Primary School, there is a clear and reliable culture around reporting issues such as compromise, loss or unethical practice. This doesn't happen on its own and needs to be taught. Again, the common sense, everyday good practice around logging out of systems when finished, having a management

plan in place if something goes wrong, and having reporting mechanisms in place also applies to using cloud technologies.

Monitoring users

Local networks based on site have the advantage of being relatively easy to filter and monitor for inappropriate or illegal use and Maendy Primary School has these systems in place. Filtering is provided as part of our school's internet provision, via the service delivered through the local authority - SRS.

Microsoft state in their user agreements that they reserve the right to actively search stored files. Maendy Primary School is clear about what the expectations are around illegal and inappropriate content and these include:

- Clear and effective agreement through a Pupil Acceptable Use of ICT Agreement and safety notice upon logon.
Positive statements around the use of technology displayed around areas where that technology might be used.
- Active education in raising awareness of what illegal or inappropriate both mean
- Staff development in recognising and escalating reports of illegal content
- Reminders that Cloud Service Providers can and do scan content stored on their servers and that an archive exists.
- One Drives provided as part of a school cloud solution will be subject to random spot checks. The system has been provided for educational use so there should not be anything in there that isn't related to learning.

Freedom of Information Act

Maendy Primary School also has a Freedom of Information Policy which sets out how it will deal with FOI requests.

Glossary

Data Protection Act 1998: All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO: The Information Commissioner's office. This is a government body that regulates the Data Protection Act.

The ICO website is here <http://ico.org.uk/>

Data Protection Act 1998: Compliance Advice. Subject access - Right of access to education records in England: General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media: General information note from the Information Commissioner on publication of examination results.

Education Act 1996: Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005: Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention

requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998: Retention of school admission and exclusion appeal papers and other pupil records.

Links to resources and guidance

ICO Guidance for schools

http://ico.org.uk/for_organisations/sector_guides/~media/documents/library/Data_Protection/Research_and_reports/report_dp_guidance_for_schools.ashx

A downloadable guide for schools

Specific information for schools is available here http://ico.org.uk/for_organisations/sector_guides/education

Privacy Notice

Privacy Notice:

Data Protection Act 1998: How we use your information

We (Maendy Primary School) are a data controller for the purposes of the Data Protection Act. At Maendy, we process personal information relating to our pupils and may receive information about them from their previous schools or pre-schools, local authority, the Department for Education (DfE) and the Learning Records Service. We hold this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

Information about our pupils that we hold will include their UPN (Unique Pupil Number), contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information.

We will not give information about you to anyone without your consent unless the law and our policies allow us to.

We are required, by law, to pass certain information about our pupils to our local authority (LA) and the Department for Education (DfE).

We are required, by law, to pass some information about you to the Department for Education (DfE). This information will, in turn, then be made available for the use by the LA.

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- our local authority at www.torfaen.gov.uk; or
- the DfE website at <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

If you want to receive a copy of the information about you that we hold, please contact via email:

- head.maendyprimary@torfaen.gov.uk