Penygloddfa CP School
General Data Protection Regulation (GDPR) Policy

1. 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

1.1 statutory requirements

It is a statutory requirement for all schools to have a Data Protection Policy: (http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a0 0201669/statutory-policies-for-schools)

1.1. Data Protection Principles

The Data Protection Act 1998 establishes eight 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.

2. 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. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school 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.

2.1. Personal data

The school has access to a wide range of personal information and data. The data is 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 e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records.
• Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
• Professional records e.g. 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.

2.2 Sensitive Personal data

Sensitive personal data is defined by the Act as information that relates to the following categories:

- race and ethnicity,
- political opinions,
- religious beliefs,
- membership of trade unions,
- physical or mental health,
- sexual life and biometric data.

It requires a greater degree of protection and in a school 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.

Note – 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, for instance in the staff room.

2.2. 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 this 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 (diary for the forthcoming year), and some of this may need to be protected by the school (a detailed scheme of work written by the school that it wishes to sell to other schools).

The ICO provide additional information on their website:
http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

3. Responsibilities

The Headteacher and Governing Body are responsible for Data Protection.

3.1. Risk Management: Roles

Data Protection Officer

Powys LA have appointed a Data Protection Officer with the responsible for the management of data protection. According to the ICO the minimum role will include:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

3.2. Risk management: Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information 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.

3.3. Risk Assessments

The school has risk assessments for all data held. An example of a risk assessment is shown in Appendix 4

4. Legal Requirements

4.1. Registration

The school has a registered Data Controller (Headteacher) on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration): http://ico.org.uk/for_organisations/data_protection/registration

4.2. Information for Data Subjects (Parents, Staff)

In order to comply with the fair processing requirements of the DPA, the school informs 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, WG, etc.) to whom it may be passed.

A privacy notice for parents / carers and pupils is shared by the school through a letter and is available on the school website.

A separate privacy notice for staff is shared by the school through a letter and is available on the school website.

5. Transporting, Storing and Deleting Personal Data

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

5.1. Information security - Storage and Access to Data

5.1.1. 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 a period of time.

- 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 clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. We fully understand the risk of data loss and the implications of a cyber attack.

5.1.2. 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 (many memory sticks / cards and other mobile devices cannot 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;
- the school allows the removal of information from site using encrypted media only;
- only encrypted removeable storage purchased by the school is allowed to be used on school computers.

5.1.3. 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.

5.1.4. Images

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

5.1.5. Cloud Based Storage

- The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example HWB, dropbox, google apps and google docs) 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.

5.2. 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 as well as data processing agreements.
  http://ico.org.uk/for_organisations/data_protection/topic_guides/data _sharing

5.3. Retention of Data

- Penygloddfa CP School has a Data Retention Schedule to ensure that data is stored for the appropriate time frame.
- Personal data that is no longer required will be destroyed and this process will be recorded.

5.4. Systems to protect data

5.4.1. Paper Based Systems

All paper based personal data will be protected by appropriate controls, for example:

- Paper based safeguarding chronologies will be in a locked cupboard when not in use
- Class Lists used for the purpose of marking may be stored in a teacher's bag.
- Paper based personal information sent to parents will be checked by Office Staff, Headteacher or Assistant Headteacher/ALNCo before the envelope is sealed.

5.4.2. School Websites

Uploads to the school website will be checked prior to publication, for instance:

- to check that appropriate photographic consent has been obtained o to check that the correct documents have been uploaded.
-

5.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

- Where technically possible all e-mails containing sensitive information will be encrypted by attaching the sensitive information as a word document and encrypting the document / compressing with 7 zip and encrypting. The recipient will then need to contact the school for access to a one-off password. The use of secure e-mail system allows for secure communication.

6. Data Sharing

Penygloddfa CP School is required by law to share information with the LA and WG. Penygloddfa CP School will ensure that, where data that is shared, it is transmitted securely for instance by secure e-mail.

7. 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 Data Protection Officer will inform the head teacher and chair of governors
- The school will follow the procedures set out in Appendix 5

8. Policy Review

This policy will be reviewed and updated if necessary every two years or when legislation changes.

Signed: ……. Janet Van Lill (Chair of Governors) **Date:** 21st May 2018

Signed: ……. Jim Macdonald (Headteacher) **Date:** 21st May 2018

Next Review due: May 2020

Appendix 1: 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

Specific information about use of Cloud Based technology
http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_comp uting

Information and Records Management Society – Schools records management toolkit
http://irms.org.uk/page/SchoolsToolkit

A downloadable schedule for all records management in schools Disclosure and Barring Service (DBS)
https://www.gov.uk/government/publications/handling-of-dbs-certificateinformation/handling-of-dbs-certificate-information

Details of storage and access to DBS certificate information. DFE Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacynotices.

DFE Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-ofchildren-in-schools

Appendix 2: Further Information

Early Years – Use of cloud based storage (e.g. Assessment Foundation)
The storage and processing of information and evidence about pupils' attainment and or classwork has changed. Some of this information is now captured electronically and stored with an external provider (Data Processor). Please inform the school office if you wish to opt out of this arrangement.

Services not Based in the EU (e.g. Google, Office 365)
Some apps/services used by the school (for example Class Dojo) transfer data to the US. The school will ensure that the company providing the app/service is certified as an approved company under the EU-US Privacy Shield. For more information - www.privacyshield.gov. Please inform the school if you wish to opt out of this arrangement.

Processing images off site (e.g. Tempest School Photography)
On occasion the school permits data to be processed off site by members of staff (e.g. Tempest School Photography). Please contact the school for further information or if you want to opt out of this arrangement.

Class Lists (e.g. class birthday lists)
On occasions the school may be asked by parents for names of children in their class. We will only share this information with parents of children in the same class. Please inform the school if you wish to opt out of this arrangement.

Appendix 3: 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.

The Information Commissioner's Office (ICO): 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.

Appendix 4: Risk Assessments

Information risk assessments, if required, 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	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk
1	SIMS Data on Pupils	Headteacher	Official	Low	Low	• Ensure Backups Complete • Ensure Data cleansing completed annually • Check password compliance
2	Safeguarding Information on Individual Pupils	Named Safeguarding Person	Official Sensitive	Low	Medium	• Ensure data passed to agencies is encrypted (e-mail) • Electronic information stored in a folder with limited, named access • Paper based information kept locked in…
3						

Appendix 5: Procedures to Report a Personal Data Breach

You must report a notifiable breach to the Headteacher (SIRO) who will then report to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must be able to give good reason for the delay. This 72 hour period includes Christmas day, bank holidays etc.

Call: 0303 123 1113 (Monday to Friday between 9am and 5pm.)

What information will I need to provide?

When you phone, we'll ask you questions about:

- what has happened;
- when and how you found out about the breach;
- the people that have been or may be affected by the breach;
- what you are doing as a result of the breach; and
- who we should contact if we need more information and who else you have told.

We'll send you a copy of the information you give us.

Here's where you can report a personal data breach to the ICO. This may include, for example, the loss of a USB stick, data being destroyed or sent to the wrong address, the theft of a laptop or hacking.

The breach will be recorded and the ICO will give you advice about what to do next.

Can I report a breach online?

If you have experienced a data breach and need to report it to the ICO but you're confident you have dealt with it appropriately, you may prefer to report online: https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc

You may also want to report a breach online if you are still investigating and will be able to provide more information at a later date.

If you are reporting online please make sure you include the telephone number of someone familiar with the breach, in case the ICO need to follow up about any of the information provided.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. So it's important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.