Cadoxton Primary School

Data Protection Policy

April 2018

DATA PROTECTION POLICY

Policy Statement

This policy outlines how Cadoxton Primary School will comply with its responsibilities under the General Data Protection Regulations.

This policy covers our acquisition, handling, processing, use and disposal of personal and sensitive data in order to provide education, it's aims, responsibilities and obligations. This includes information on current, past and prospective pupils, parents, permanent and temporary staff, volunteers, Governors, contractors, partners and others who come into contact with the school.

Personal Data

Personal information will be used as set out in line with the General Data Protection Regulations. It includes reference to personal information kept on paper, computer or recorded on other material.

Personal data is any information about a living person who can be identified by their name, address, online identifier such as an IP address, school activities, attendance record, behaviour tracking, bank details and/or financial information in relation to parents and/or guardians, additional learning needs, attainment, images, references or expressions of opinion about them.

It is data that has been, or will be word processed or stored electronically, e.g. computer databases and CCTV recordings, personal information that is, or will be kept in a file which relates to an individual or in a filing system that is organised by reference to criteria which relate to the individuals concerned, e.g. name, school year, school activities.

Sensitive personal data is any information about a person's mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings.

As a school we have additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied:

- explicit consent of the data subject must be obtained
- necessary for carrying out the obligations under employment, social security, or social protection law or a collective agreement
- used in connection with ex-pupils / ex-staff provided it relates solely to them and there is no disclosure to a third party without consent

- data manifestly made public by the data subject
- various public interest situations as outlined in the General Data Protection.

Nature of Personal Data

Data Subject	Nature of Data	Location	Access
Pupils	Address, phone contact details, Emergency contacts	Administration office	Staff
Staff, Contacts	Address, phone contact details, Emergency contacts, email addresses	Administration office	Administration Staff Staff through request
Pupils, Staff, Parents and Guardians	SIMs PLASC	Administration office	Headteacher, Administration staff via password
Pupils, Staff	Tracking data, Equality, Bullying and ESafety Logs	Headteachers' office	Headteacher and Teachers through consent
Parents and Guardians and General Public	Compaints Log	Headteachers' office	Headteacher and with access consent
Pupils	Individual assessment data	Class files and on personal computers and within Building Blocks	Teachers, individual passwords
Pupils, Parents and Guardians	Safeguarding	My Concern, computer	Individual staff passwords, allocated access
Pupils and staff	Medical Information	SIMS, Admin. office	Headteacher, Administration staff via password
Pupils	Medical Log	Cwtch	Cwtch staff, Staff
Staff, Parents and Guardians, Visitors	Accident book	Administration office	Staff
Pupils	Additional Learning Needs	ALN room	ALNco
Staff	Job descriptions, contracts and performance management	Headteachers office	Headteacher and SLT
Governors	Contact details	Headteachers office in file, Personal computer	Headteacher and Administration staff, PC via password
All	24hr CCTV	School perimeter	Headteacher, Adminstration staff, Caretaker

Roles and Responsibilities

- As a school we are the ***Data Controller*** of personal information for the purposes of the Act. As part of this role it is our duty to notify the Information Commissioner's Office, as the regulator, of the personal information being processed. This is completed online: https://www.ico.gov.uk/onlinenotification/?page=7.html

- All staff have responsibility for ensuring the security and safekeeping of the personal information held.

- Day to day responsibility for ensuring the implementation of this policy will be undertaken by the Senior Leadership Team, which in turn will be supported by the Governing Body.

- The Data Protection Officer will ensure that staff are annually updated with any changes to the policy and that all new staff are trained in compliance. See Appendix 1

- The staff handbook contains a section on Data Protection for staff, volunteers, students and supply staff.

- Overall responsibility for data protection has been delegated to Valerie Tattersall, who is the School's ***Data Protection Officer*** and will report to the Governing Body.

- A record of internal processing activities is maintained in the context of a Data Map, see Appendix 2. Clear, comprehensive and transparent privacy policies and procedures will be maintained.

Intentions

The lawful and proper treatment of personal information is fundamental to the effective delivery of our objectives and as key to the maintenance of confidence between our school and its pupils, staff and parents. It is our intention that the eight ***'data protection principles'*** are adhered to.

Principle 1: ***Personal data will be used fairly and lawfully.***

When we as a school acquire personal information that will be kept as personal data, we will be fair to the data subject and to whoever provides the information, data will be handled and safeguarded in compliance with the Act.

Principle 2: ***Personal data will only be used for purposes that are specifically stated.***

If information has been obtained for one purpose it cannot be used for a secondary purpose.

Principle 3: ***Information will be adequate, relevant and not excessive.***

Principle 4: ***Information will be accurate and up to date.***

As a school we will record information accurately and will keep it up to date as need arises and through general annual school data collections. This will include personal contact and medical information.

Principle 5: ***Information will not be kept for no longer than is necessary.***

Retention of personal data will be in line with our Retention Policy, See Appendix 3.

<u>Principle 6:</u> Information will be processed according to data subjects' legal rights.

<u>Principle 7</u>: Information will be kept safe and secure.

- School's premises are alarmed & data locked away.
- Computer systems being operated by the school are all password protected. Staff and pupils are reminded to change their passwords at regular intervals. All School laptops have passwords changed regularly.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices if they contain sensitive data.
- School's equipment i.e. computers, laptops & electronic storage devices are wiped by the our ICT providers before being destroyed or reused elsewhere.
- Paper records which include confidential information are kept in a cabinet, or office which is locked when unattended.
- Personal data stored on computers is file encrypted, anti-virus and security software installed, and sufficiently robust and frequently changed passwords are used.
- Personal data is not removed from school premises unless stored in an encrypted form on a password protected computer or memory device.
- Staff must not leave or use computers, memory devices or papers where there is a significant risk that they may be viewed or taken by an unauthorised person, they should not be viewed in public, left in a car, where risk of theft is greater.

All staff are made aware of the following additional requirements:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal information are kept in a secure location when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will cross-shred or incinerate paper-based records
- Staff adhere to the school's practices and procedures in respect of personal information, e.g. sharing information with third parties, home working, staff awareness of the Data Protection Act.

<u>Principle 8</u>: Information is not transferred outside the European Economic Area without adequate protection.

Personal data will not be transferred outside the European Area (EEA) without the data subjects permission or unless it is satisfied that the data subjects rights will be adequately protected and transfer has been approved by the Data Protection Officer.

Lawful Basis for Processing Data

Personal information will only be processed where there is a lawful basis for doing so.

- To provide all pupils and staff with a safe and secure environment.
- Safeguarding and promoting the wellbeing and welfare of all pupils and staff.
- To fulfil our contractual and other legal obligations as a school.
- To provide and education, professional development and pastoral care.
- To provide activities, enrichment and trips for pupils, parents and carers.
- To provide academic and professional development information and references for pupils and staff.
- Promoting and protecting our interests and objectives as a school.
- For personnel, administrative and management purposes, e.g. paying staff, performance.

Privacy Notices

Our Privacy Notice informs data subjects of what data is collected and what it is used for. Our school privacy notice can be accessed on our School website and within Appendix 4 of this policy.

Individual Rights

We regard individuals' rights as fundamental and therefore endorse the enhancement of individual data rights as set out in the legislation. All requests for personal information will be dealt with in accordance with the individual's statutory rights and on a case by case basis. The GDPR provides the following rights for individuals:

1. The right to be informed (Privacy notices).

2. The right of access

Exemptions – to the Right of Access

The Data Protection Bill introduces exemptions to the Right of access as follows;

- The right to obtain personal information (subject access) is exempted in respect of Education Data if its release would be likely to cause serious harm to the physical or mental health of the data subject or another individual.
- The right of access does not apply to child abuse data to the extent that the application of the provision would not be in the best interests of the data subject. Child abuse data includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of an individual aged under 18. It consists of data whether they have been subject to or may be at risk of Child abuse.
- The right of subject access is exempted in respect of statements of special educational needs where disclosure is prohibited or restricted under the law governing special educational needs and disability. Equally the right is exempted where prohibited or restricted under the Adoption and Children Act 2002 and the Human Fertilisation and Embryology Act 2008.

3. The right to rectification

4. The right to erase

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete. Where a request for rectification is received, the statutory time limit is one month. This can be extended by two months where the request for rectification is complex.

The right to erasure is also known as "the right to be forgotten" and enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

5. The right to restrict processing

6. The right to data portability

7. The right to object

8. Rights in relation to automated decision-making and profiling.

Disclosing personal information beyond school

Sharing of personal data is often permissible as long as doing so is fair and lawful under the Act. However, the Data protection officer should be contacted if in doubt.

Response to telephone calls for personal data:

- End the call, and phone the relevant central switchboard asking to speak with the person making the request.
- Ensure they are able to share the information and that the necessary consent is in place.
- Ensure adequate security. What is adequate will depend on the nature of the data.

Photographs

- Consent is required every time names are used alongside photographs.

Contracts / Data Sharing

- As a school we will comply with the further requirements, for third party processing, as set out in Article 28 of the GDPR. We will only appoint contractors who can provide "sufficient guarantees" that the requirements of the GDPR will be met and the rights of individuals are protected.

Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This means that a breach is more than just losing personal data, for example, unauthorised access is also a breach. E.g. Sending an email to the wrong person by mistake, loss or theft of IT equipment containing personal data, loss or theft of hard copies of hard data, failing to deal with subject access requests.

- If a personal data breach has occurred, we as a school have 72 hours from the time we become aware of the breach, to report it to the Information Commissioner's Office unless the breach is unlikely to result in a risk to the rights of data subjects. If the breach is likely to result in a high risk to the rights and freedoms of individuals, they will be informed without undue delay.

Data Access Requests (SAR)

- As a school we have 30 days to respond to a Subject Access Request from whenever it is received.

Compliance Status

- Compliance with this policy is mandatory for all staff who have access and use of personal Information. Breach of this policy by employees may be regarded as gross misconduct and may lead to termination of employment.

Policy Review

- This policy has been prepared as of April 2018. At that point the Data Protection Bill is progressing through Parliament. This policy will be reviewed when the Bill is finalised.

Signed School Representative: _____

Signed Governor Representative: _____

Date: _____

Appendix 1: Staff training and Compliance Procedures

- Annual training or on joining school.
- ICO recommends 1 ½ to 2 hours training annually.
- Termly briefings / Compliance reviews

Training Agenda

- Policy introduction / review

Content for discussion / compliance:

- Lock personal documents away and keep the key secure
- Clear desk and work area of information when you leave the room.
- Ensure that when any information is passed to a third party, they are aware of safe storage of this information.
- When leaving your laptop / computer / device momentarily, lock your machine or log out in order to prevent unauthorised use of your machine.
- Lock laptops away when not in use or use a Cable lock if it is to remain on your desk.
- Protect your computer with encryption software
- Change passwords regularly and user lower, upper case and numbers.
- Use encrypted storage devices.
- Store removable media securely.
- Encrypt data stored on CD-R/W

Working at Home

- Follow risk assessments.
- Be aware of your obligation to ensure home equipment is proven to be secure.
- Satisfy yourself that in the unfortunate event of the computer being lost or stolen the information held on the computer cannot be extracted.
- Ensure that any email or online storage containing personal data is secure and that the physical data storage and servers are located within the EEA
- Don't post information on the wall if it is visible through a window.
- Don't post information or have information visible to any person(s) who should not see it such as in a staff room where a pupil or other individual may visit.
- Don't leave information on view in a car/at home.
- Don't give out information to a person (even over the phone) without independently verifying this person's identity and their right to the information.
- Don't leave a laptop unattended or allow unauthorised people to use the laptop.
- Don't share passwords, write them down or save them in web browsers.
- Don't use obvious passwords such children's or pet's names.
- Don't leave discs in a car/handbag/pocket or use non encrypted removable media (USB, CD-RW, etc).
- Don't send emails to a personal computer at home unless that computer is encrypted.

- Don't allow family members to access the personal information being held.

Online Security

- Do ensure your computer is updated regularly with security software.
- Do respond appropriately to onscreen warnings. Note that a
- warning on the screen may actually be a harmful website imitating a Windows message. Ask your IT Support colleagues if you are unsure, before clicking "OK"
- Do report incidents of „phishing. (emails which request personal information)
- Do try to only use the schools contacts or address book. This will minimise the risk of information being sent to the wrong recipient in error.

- Don't install software without having it approved.
- Don't download files or programs if you cannot first verify the source.
- Don't click on links in unsolicited emails, especially if the email requests confirmation of personal information such as passwords.
- Don't turn off any built-in email security measures i.e. Spam filters.
- Don't Email sensitive information such as pupil spreadsheets, unless encrypted.
- Don't bypass security measures by emailing personal information to another non- secure computer.
- Members of staff will be made aware of the school's password policy at induction, through the school's e-safety policy and password policy through the Acceptable Use Agreement.

Pupils

- Pupils will be made aware of the school's password policy in ICT, PSHE and e-safety lessons, through the use of posters placed around the school and through the Acceptable Use policy

CCTV

- CCTV is only used for access screening to main doors/gates and security of site.

Photographs/Media Images of Children

- The Data Protection Act does not prohibit taking photographs of the children by family members, such as parents, grandparents and carers.
- In regards to the Data Protection Act, it is acceptable for parents to take photographs during the school sports day or music concert.
- Consent is obtained from all parents/carers prior to the school taking photographs for official purposes such as I.D. Cards, Prospectus or for publicity purposes.
- Parents are informed that photography for media and/or promotional purposes occurs periodically and that they should advise the head teacher if they wish their child to be excluded from these activities.
- Under the DPA 1998, individuals have rights in relation to the use of their photo, the most relevant being their right to withdraw consent to its publication at any time and their right not to have it

used for any purpose other than that stated clearly on the consent form, e.g. display on the Web site, use in promotional literature etc.

- Pupils' names should not be included in any photograph that may be accessed by the public.

- Record of staff training and reviews.

Appendix 2: Data Mapping

In process

Cadoxton Primary Data Map

What data?	Where is the data kept?	Why is the data kept?	Where does the data come from?	Permission
Employees Name, email, phone number, address, DoB, Bank details, Emergency contacts	SIMS Email Finance System Payroll System	Contact Pay Emergencies	Employee	Contract of employment
Parents Name, email, phone number, address, Facebook group,		Contact regarding child illness Concerns regarding child, e.g. attendance, punctuality, Rising incidents and issues. Newsletter sent weekly Emergency information & updates, e.g. cancelled clubs, events	Parents	Consent updated each academic year
Children Name, DOB, address, phone number, parental / guardian information, HWB Email addresses, Mathletics passwords, Bug Club passwords, See-Saw passwords, UPN, Baseline Data, WG Test data, NV test data, Attainment records, ALN information regarding interventions, support and	SIMS DEWI site S2S site Printed contact details folders Class data files Class password folders Class Blue Folders	Contact Safeguarding Overview of passwords used UPN data identification Sustained progression Full history from multi agencies to ensure child is supported and safeguarded	Parents LEA Welsh Government Other Schools Children's Services	Consent updated each academic year
involvement of outside agencies, Information from Children's Services, associated PPN reports,	Private / Confidential letters – ALN / Safeguarding Co-ordinator My Concern Teachers folders - laptops		Pupil Support Services Health Services Police	
What data?	**Where is the data kept?**	**Why is the data kept?**	**Where does the data come from?**	**Permission**
Governors Name, email, phone number, address				
Suppliers				

Appendix 3: Retention Policy

In process

Appendix 4: Privacy Notice shared with parents / guardians

Privacy Notice

To meet the requirements of the Data Protection Act 1998, schools are required to issue a Privacy Notice to pupils and/or parents summarising the information held on record about pupils, why it is held, and the third parties to whom it may be passed.

This Privacy Notice provides information about the collection and processing of pupils' personal and performance information by the Welsh Assembly Government, **Vale of Glamorgan** Local Authority (LA) and **Cadoxton Primary School**.

The collection of personal information:

The school collects information about pupils and their parents or legal guardians when they enrol at the school. Information is also received from other schools when pupils transfer.

The **School** processes 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' educational progress;
- the provision of welfare, pastoral care and health services;
- the giving of support and guidance to pupils, their parents and legal guardians;
- the organisation of educational events and trips;
- planning and management of the school.

Welsh Government (WG) & Local Authority (LA)

The Welsh Assembly Government receives information on pupils normally as part of what is called the Pupil Level Annual Schools Census (PLASC).

The Welsh Government uses this personal information for research (carried out in such a way that ensures individual

pupils cannot be identified) and for statistical purposes, to inform, influence and improve education policy and to monitor the performance of the education service as a whole. Examples of the sort of statistics produced can be viewed at www.wales.gov.uk/statistics

The LA also uses the personal information collected via PLASC to do research. It uses the results of this research to make decisions on policy and the funding of schools, to calculate the performance of schools and help them to set targets. The research is carried out in such a way that ensures individual pupils cannot be identified.

In addition, the Welsh Government and LAs receive information regarding National Curriculum assessment and Public Examination results and attendance data at pupil level.

The nature of personal information that will be held includes:

- personal details such as name, address, date of birth, pupil identifiers and contact details for parents and guardians;
- 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.

Organisations who may share personal information:

Information held by the School, LA and the Welsh Government on pupils, their parents or legal guardians may also 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 Welsh Government, 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 regulators and inspection authorities, where the law requires that information be passed on so that they can do their work.

Pupils have certain rights under the Data Protection Act, including a general right to be given access to personal data held about them. The presumption is that by the age of 12 a child has sufficient maturity to understand their rights and to make an access request themselves if they wish. A parent would normally be expected to make a request of child's behalf if the child is younger. If you wish to access your personal data, or that of your child, then please contact the relevant organisation in writing.

Details of these organisations can be found on the following website: http://www.valeofglamorgan.gov.uk/our_council/freedom_of_information.aspx or for those pupils/parents where this is not practical, a hard copy can be obtained from the school secretary.

Other information

The Welsh Government, LA and school place a high value on the importance of information security and have a number of procedures in place to minimise the possibility of a compromise in data security. The Welsh Government, LA and School will endeavour to ensure that information is kept accurate at all times. Personal information will not be sent outside the United Kingdom.

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 on **you**, 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 if an organisation does not comply with the Data Protection Act 1998 and you person suffer damage;
- 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 its' 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;

- School on **01446 741518**
- LEA on **01446 700111;**
- The Welsh Government's data protection officer at, The Welsh Government, Cathays Park, Cardiff, CF10 3NQ;
- The Information Commissioner's office help line can be contacted on 01625 545745
- Information is also available from www.ico.gov.uk.

Appendix 5: Audit Check List

1. Has the school notified the Information Commissioner's Office of the nature and type of information it is processing?
2. Has this guide been circulated to all staff?
3. Has the school appointed an Information Asset Owner or Data Protection Lead?
4. Does the school provide a Privacy Notice or Fair Processing Notices to individuals at the time of collecting personal information?
5. Does the school regularly evaluate the accuracy of the information it retains?
6. Does the school have recognisable and accessible Retention Schedules?
7. Are all computers, laptops, USB memory sticks and other storage devices, such as discs using approved encryption technologies?
8. Is personal information removed from the premises? For example, for the purposes of working from home, are staff aware of their obligation to keep this information secure?
9. Is the information retained in paper files stored securely?
10. Is sensitive or confidential information subject to restricted access?
11. Is personal information disposed of in a secure manner?
12. Does the school send personal information to any third party organisations? If so, the school must have a written agreement with that third party confirming that the information (being shared) is kept securely and that it will only be used in accordance with the school's instruction.
13. Has the Data Protection Lead member of staff received an appropriate level of training in respect of the Data Protection Principles?
14. Has the Data Protection Lead provided training to the staff at your school?
As a guide, the ICO recommends staff undertake approximately 1.5 to 2 hours training annually.