A nurturing inclusive learning community that enables everyone to be their best

CALTON PRIMARY SCHOOL

CALTON PLAYGROUP

CALTON PRIMARY SCHOOL AND PLAYGROUP

GENERAL DATA PROTECTION REGULATIONS

Approved by Leadership, Management and Premises LMP Committee on 29/11/2021

Next renewal date: LMP Term 2 22/23

This policy links to:
Freedom of Information Policy

Contents Page

1. Introduction

In order to work effectively Calton Primary School ("the School") has to collect and use information about people with whom it works. This may include (past, present and future) pupils, parents, teachers, trustees, members of the public, contractors and suppliers. In addition we may be required by law to collect and use information in order to comply with the requirements of central government.

All personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it is on paper, in computer records or recorded for other means. We are all responsible for its safe handling.

This documents sets out the principles of data protection, our responsibilities, the access rights of individuals as well as information sharing and complaints.

2. Scope/ Our Commitment

This policy applies to all staff, governors, contractors, agents, representatives and temporary staff, working for or on behalf of the School. The requirements of this policy are mandatory for all of these parties.

The School regards the lawful and correct treatment of personal information as critical to its successful operation, maintaining confidence between the

school and those it interacts with. The school will ensure that it treats personal information correctly in accordance with the law.

The School fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

The school is committed to ensuring that their staffs are aware of data protection policies, legal requirements and that adequate training is provided by Gloucestershire County Council.

Changes to data protection legislation under the GDPR and DPA, shall be monitored and implemented in order to remain compliant with all requirements.

3. Principles of data protection

The GDPR outlines seven key principles for anyone who processes data. These principles form the basis of our approach to processing personal data.

Guide to data protection | ICO link takes you to the principles on the ICO website

Key definitions of the Data Protection Act | ICO (takes you to definitions of personal data)

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive and is accurate.
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

4. Responsibilities

The School is registered as a data controller with the ICO and will renew this registration as required.

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Register of data controllers | ICO
Data breaches shall be notified within 72 hours to the individual(s) concerned and the ICO.

The members of staff responsible for data protection within the School are the Headteacher and the School Business Manager. However, all staff must treat all pupil (or other relevant) information in a confidential manner and follow the guidelines set out in this document.

We have appointed Gloucestershire County Council as our Data Protection officer. They can be contacted on 01452 583619 or schooldpo@gloucestershire.gov.uk

5. Definitions of Data

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual but need not be sensitive information. The GDPR makes a distinction between personal data and "special category" (sensitive data). Special category personal data requires stricter conditions for processing.

Personal data is defined as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller' (the School is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.

Special Category Data is information about racial or ethnic origin, sexual life or sexual orientation, biometric and genetic data, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.

6. Processing Personal Data

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law. When special category

personal data, criminal conviction data or data about offences, is processed, a lawful basis and additional condition will be satisfied.

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

7. Fair Processing / Privacy Notice

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of an individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

8. Sharing data

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health.

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Any proposed change to the processing of individual's data shall first be notified to them.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**

If a pupil transfers from Calton Primary School to another school, their records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Education division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition

- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

9. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, prospectuses newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns or third party benefactors (such as charities or companies who provide financial support to the school).
- Online on our school website or social media pages/ feeds.
- Videos and photographs may be labelled with pupil's names or tutor groups when used in this way.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

10. Data Protection rights of the individual

Data Access Requests (Subject Access Requests)
All individuals, whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

The Head Teacher
Calton Primary School
Calton Road
Gloucester
GL1 5ET

No charge will be applied to process the request.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- Where personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

11. Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO: Risk and impact assessments | ICO

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

12. Location of information and data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard or office. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical officer.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly locked or shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers
- Laptops that staff use must be password protected
- Staff must not use portable memory devices or similar to hold any data relating to School. The School provides staff with access to network files remotely through Foldr: https://foldr.caltonprimary.co.uk
- Staff working remotely must ensure that they take the appropriate actions to keep School data safe.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

13. Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance: IT asset disposal for organisations | ICO

The school has identified a qualified source for disposal of IT assets and collections. The school also uses Print Waste to dispose of sensitive data that is no longer required.

14. Complaints

Complaints about how the school processes data under the GDPR and responses to subject access requests are dealt with using the School's complaints procedure.

15. Breach of Policy

Any breach of this policy should be investigated in accordance with our Data breach process The School will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.