Coombe Bissett CEVA Primary School

'Within a caring Christian community we enable every child to flourish and inspire a love of learning in all members of our community'

General Data Protection Regulations (GDPR) Policy

Introduction

Coombe Bissett CE VA Primary School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA). This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements. The legal bases for processing data are as follows:

(a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.

(c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

Further information is may be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/

The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.
The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The members of staff responsible for data protection are mainly Deborah Cockrean (Head Teacher) and Michelle Fiander (Admin Officer). However all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.

The school has a Data Protection Officer, Mr Wesley Thorpe, Headteacher at Alderbury and West Grimstead Primary School who may be contacted at Alderbury and West Grimstead Primary School.

The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

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

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;

4. Personal data shall be accurate and where necessary, kept up to date;

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data held.

Duties

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.
Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the Data Controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this
- If the school plans to transfer personal data outside the EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures.

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.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the school is required either by law or in the best interests of our students 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.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

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

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:
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/

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.

Data Access Requests (Subject Access Requests)

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within 20 working days (excluding the summer holidays, Christmas and Easter holidays) and they should be made in writing to: Mr Paul Lailey (Head Teacher)

No charge will be applied to process the request.

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 Coombe Bissett CE VA Primary School to another school, their academic 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.

Educational 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.

Right to be forgotten

Where any 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.

Photographs and Video

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources. It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent and should not then share these images on any form of social media (including but not limited to: Facebook, Instagram, Twitter, Snap Chat, WhatsApp, LinkedIn etc).

Location of information and data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. 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 shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be downloaded onto a secure USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.
- USB sticks that staff use must be password protected. 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.

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 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: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf
The school has identified a qualified source for disposal of IT assets and collections.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Procedure in the event of a data breach

The Data Controller (Deborah Cockrean) is told of breach and this is recorded. The Data Controller will inform the Data Protection Officer (Louse Knipe). If deemed serious the Data Controller will inform the people whom the breach affects immediately, or as soon as possible after the breach. The Data Protections Officer will investigate the incident and have all the relevant and facts to establish a time line of events. The Data Protection Officer and the Data Controller may make recommendations for changes in procedure so that the type of breach does not occur again. Any documents that have been sent to the wrong person must be recalled.

The Data Protection Officer then has 72 hours in which to report the breach to the ICO (if deemed serious) and complete the online form on the ICO website. A response case number received by email from the ICO will be retained with the information of the breach.

The Data Protection Officer and the Data Controller will ensure that all people affected by a breach are informed of the process and, if appropriate, what measure have been put in place.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years. The policy review will be undertaken by the Data Protection Officer, Head teacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Mrs Deborah Cockrean.

Related documents

Complaints Policy
Privacy Notice – School Workforce
Privacy Notice – Pupils
Privacy Notice Volunteers including Governors
Consent form
Information sharing agreement with the Friends (Parent Group)

Effective Date	Reason for change or revision	Authored/reviewed by	Next review date
May 2018	Implement GDPR legislation	D Cockrean	Initially after 1 year and then 3 years
October 2018	Inclusion of process in case of data protection breach	D Cockrean	October 2019