The Colleton Primary School
Colleton Drive
Twyford
Berkshire
RG10 0AX

T (0118) 934 0530
F (0118) 934 4641
E admin@colleton.wokingham.sch.uk
www.colleton.wokingham.sch.uk

Data Protection Policy

1. Introduction
    a. Our school is committed to protecting all data that it holds relating to staff, pupils, parents and governors.
    b. This policy applies to all school data, including CCTV, regardless of whether it is in paper or electronic format and where it is stored.
    c. This policy was approved by governors on 12th May 2021 and will be reviewed annually.

2. Legislation and guidance
    a. This policy meets the requirements of the Data Protection Act 2018 (which incorporates the UK General Data Protection Regulation) and is based on guidance published by the Information Commissioner's Office (ICO) and the Department for Education. All staff and governors should note that the Act makes provision for significant fines to be levied in the event of non-compliance.
    b. Section 6 also refers to the Education (Pupil Information) (England) Regulations 2005.
    c. Section 7 refers to the Freedom of Information Act 2000.

3. Data protection principles and categories of data
    a. The Data Protection Act 2018 sets out six data protection principles that the school must follow when processing personal data. Data must be:
        - Processed fairly, lawfully and in a transparent manner
        - Used for specified, explicit and legitimate purposes
        - Used in a way that is adequate, relevant and limited
        - Accurate and kept up-to-date
        - Kept no longer than is necessary
        - Processed in a manner that ensures appropriate security of the data.

    b. Categories of data
        i. The Data Protection Act 2018 refers to **Personal data** and **Special categories of personal data.**
            - **Personal data** means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

- **Special categories of personal data** (previously known as 'sensitive personal data') includes race, ethnic origin, politics, religion, trade union membership, biometrics, health and sexual orientation.

ii. We note that the DfE consider it best practice that data such as free school meal status, pupil premium eligibility, elements of special educational need information, safeguarding information, some behaviour data and Children's Services interactions are also treated with the same care as the special categories set out in law.

4. Roles and responsibilities
   a. The Data Controller
      i. Our school processes personal information relating to pupils, staff and visitors (defined as 'Data Subjects') and is therefore a Data Controller.
      ii. The Governing Body has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 2018.
      iii. The Headteacher will ensure the provisions of this policy are in place and that all staff are aware of their data protection obligations.
      iv. Day to day responsibility for Data Protection will reside with the Data Protection Officer (DPO).
      v. The school is registered as a Data Controller with the ICO and renews this registration annually.
   b. Data Protection Officer
      i. The Data Protection Officer will:
         - Act as the contact point for all Data Protection issues and queries from Data Subjects and the ICO, e.g. for Subject Access Requests, data breaches, following the agreed procedures (see Appendix b)
         - Maintain appropriate documentation related to data processing
         - Undertake the training necessary to fulfil their role, and ensure staff have access to appropriate training and updates
         - Monitor compliance with all aspects of Data Protection
         - Provide advice relating to Data Protection Impact Assessments (DPIA) e.g. before introducing a new data processing system.
   c. School staff
      i. All school staff, in whatever role, have a duty to comply with this policy. Failure to comply may result in disciplinary action.
      ii. Staff must report any data related concerns or breaches immediately to the DPO.
      iii. Staff must complete the prescribed training on our data protection policies and procedures in a timely manner.
   d. Data processor

      The school uses a range of third parties to process data on our behalf, e.g. payroll, catering, communications. We will use our best endeavours to ensure that third parties have a written contract in place that establishes the purpose and manner that personal data will be processed; processor's security arrangements are adequate (at a minimal equivalent to what we have) and take reasonable steps to ensure compliance with those obligations.

e. Sharing data
    i. Where data is routinely shared with other organisations (e.g. Local Authority, DfE, NHS, Police) the school will ensure this is made clear in the Privacy Notice and that appropriate protocols are in place.

5. Data Protection documentation
    a. Privacy Notices
        i. The school will make available Privacy Notices for Pupils/Parents, Staff and Governors that set out how the school will make use of their personal data. These will be made available via the school website.
    b. Consent
        i. Where required the school will seek and record specific consent from data subjects (e.g. image permissions, marketing, biometrics).
    c. Data Protection Audit/record keeping/logs
        i. The school will maintain suitable records which detail all data that is collected, processed and where appropriate shared. The Key audit tool will be used for this purpose. In addition, the school will keep records of other key areas including:
            - Subject Access Requests – see Appendix (b)
            - Data Breaches – see Appendix (a)
            - Data retention schedule, disposal/destruction log
            - DPIA
            - Requests for changes to data
            - A general description of the technical and organisational security measures that are in place
            - Staff training on data protection procedures
            - Device and systems acceptable use agreements by pupils / parents and staff.

6. Subject Access Requests/Parental requests to see the educational record
    a. Under the Data Protection Act, pupils (or their parents for children under 13) have a right to request access to information the school holds about them. This is known as a Subject Access Request (SAR).
    b. The SAR process and timescales are provided in Appendix (b).
    c. In addition, we are aware of Regulation 5 of the Education (Pupil Information) (England) Regulations 2005 that gives parents the right of access to their child's educational record, free of charge, within 15 school days of a request.

7. Freedom of Information Act (FOI)
    a. The school will comply with the Freedom of Information Act 2000. The school has a separate Freedom of Information policy which is published on the school website. Any freedom of information requests will be dealt with in accordance with that policy.

8. Security and storage
    a. The school will ensure that appropriate technical and organisational measures are in place to protect school data.

b. The school will ensure that staff and governors are only able to access data that is relevant to their role.
c. The school will ensure that staff and governors are provided with specific guidance, which should include for example:
    - Use of encrypted USB flash drives/memory sticks and other removable media
    - Appropriate use of professional and personal email accounts
    - Use of encrypted/Secure email
    - Secure storage of paper files, clear desk policies, etc
    - Screen locking procedures
    - Use of cloud based storage
    - Taking data off site/Home working
    - Use of staff personal devices
    - Passwords
    - Encryption of school devices that may be taken off site, e.g. staff laptops.

d. Key points from the list above will be included in Staff Acceptable Use Agreements.

9. Retention and disposal
    a. The school will produce a document retention and disposal schedule. This will be based on the retention guidelines from the Information and Records Management Society (IRMS) Toolkit for Schools and any other guidance, e.g. DfE, Local Authority, local agreements.
    b. Appropriate measures will be taken to ensure that data that is no longer required, whether in paper or electronic form, is disposed of securely.
    c. The school will ensure appropriate disposal of all devices that hold school data.
    d. A destruction record will be kept for all data and devices that are disposed of.

10. Training
    a. All staff and governors will be provided with data protection training as part of their induction process.
    b. Data protection training, briefings and updates will also be provided for all staff and governors as required, but at least every two years.

11. Protection of biometric information
    a. We do not have or use a biometric recognition system.

Responsibility: Staff and Finance Committee/Data Protection Officer
Reviewed: Spring term 2021
Approved by the Full Governing Body: 12th May 2021
Next review: May 2022

Appendix

(a) Data breach information and procedures

Data protection breaches can be caused by a number of factors, e.g. Loss or theft of pupil, staff or governing body data and/or equipment or paperwork on which data is stored, inappropriate access controls allowing unauthorised use, poor data destruction procedures, human error such as sending an email to the wrong person, cyber-attack, hacking, ransomware.

In the event of a breach, the procedures below are to be followed:

1. Any data protection incident is to be reported immediately to the school's DPO and Headteacher.
2. If required, appropriate actions will be taken to halt the breach, and/or prevent further breaches.
3. The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.
4. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

    If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible. If in doubt as to the significance of the incident, we may seek external advice, which could involve contacting the ICO.

    The Chair of Governors will be informed as soon as possible. Other agencies as appropriate may need to be informed depending on the breach, e.g. police, Action Fraud, social services.

5. Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
6. The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
7. The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure.)
8. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
9. We will fully investigate the breach, and review all related policies and procedures to make any necessary changes.
10. Provide additional training to staff as appropriate.
11. Review whether any disciplinary action should be taken.
12. If the nature of the breach could result in adverse publicity we may wish to prepare a statement for publication.
13. A full record will be kept of all data breaches, including all the steps taken, whether reportable or not.

Additional notes

In the event of a data breach, the following areas will be considered:

- The type of data and its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

(b) Subject Access Request (SAR) process and timescales

A SAR is a request for personal data about the applicant but the right of access goes further than this and individuals have a right under data protection laws to:

- know whether their personal information is being processed (which includes being held or stored)
- be given a description of the data held, the purpose for which it is processed and to whom the data may be disclosed
- be given a copy of the information held
- be given information as to the source of the data.

Where pupils are under the age of 13, a SAR will be made on their behalf by the parent/guardian or their legal representative.

SARS can be made in writing, verbally or through a social-media portal. An individual may ask a third party (e.g. a relative, friend or solicitor) to make a SAR on their behalf. Before responding, the school need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

1. Clarify that this is a SAR and not some other request for information, i.e. a FOI request or an 'educational record' request.
2. Confirm the identity of the person making the request. Examples of suitable documentation are valid passport, driver's license, birth certificate along with some other proof of address (e.g. a named utility bill) or information that is only known to the organisation and subject. Methods of identification will not exceed the level of personal data held by the school.
3. If it is unclear what information is being requested, we will ask for further details from the applicant.
4. Check that the information is available:
    - If the information is not available, we will inform the applicant.
    - If the information is available, we will note the date that the SAR was received and identity of the person making the requests was confirmed or, in the case of further details being requested, the date that these were received. The school has 28 days to respond.
5. Check that the information requested does not infringe on any data protection exemptions that may apply (as outlined in the DPA 2018).
6. We will check whether the information requested contains information about any third-party. If it does then we will undertake one, or more, of the following steps:
    - Seek permission to disclose the information from the third-party concerned.
    - Redact/summarise the information to protect the identity of the third-party.
    - Withhold the information to protect the rights of the third-party.
7. We will ensure that the information to be supplied is clear and understandable, e.g. any complex codes or terms are explained.
8. Supply the information requested in an appropriate format, e.g. if the request is made electronically, the information should be provided in an electronic format.

9. Keep a record of the SAR and any information that was supplied. Where any redactions are made, an un-redacted version of the request will be retained by the school and presented to the ICO if requested.

Additional notes

- The school will provide a copy of the information free of charge. However, we reserve the right to refuse or apply a 'reasonable fee' for requests that are deemed to be a duplicate request, manifestly unfounded or excessive. We may also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information.
- We will be able to extend the one month period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the applicant within one month of the receipt of the request and explain why the extension is necessary.
- We might also decide to withhold some information. Examples of some information which (depending on the circumstances) it might be appropriate to withhold include:
    - information that might cause serious harm to the physical or mental health of the pupil or another individual
    - information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
    - information contained in adoption and parental order records; and
    - certain information given to a court in proceedings concerning the child.
- Anyone with full mental capacity can authorise a representative/third party to help them make a subject access request, for example solicitors/advocates. Before disclosing any information, the school must be satisfied that the solicitor/advocate has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included.
- More information about SARs is available on the ICO website.
- If an individual is dissatisfied with the way their subject access request has been managed, they should be advised to invoke the CCGs' complaint process. If they are still dissatisfied, they can complain to the Information Commissioner's Office. This can be done in writing to: Information Commissioner's Office Wycliff House, Water Lane, Wilmslow, Cheshire, SK9 5AF.