

# Data Protection Policy

---

## 1. General Statement

The Principal and Governors of this College intend to comply fully with the requirements, and principles, of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

## 2. Enquiries

Information about the College's Data Protection Policy is available from the Principal. General information about the Data Protection Act can be obtained from the Data Protection Commissioner.

## 3. Fair Obtaining and Processing

Frome College undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

"processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

"data subject" means an individual who is the subject of personal data or the person to whom the information relates.

"personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

"parent" has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

## 4. Registered Purposes

The Data Protection Registration entries for the College are available for inspection, by appointment, at the College Main Reception. Explanation of any codes and categories entered is available from the Principal who is the person nominated to deal with Data protection issues in the College. Registered purposes covering the data held at the College are listed on the College's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

## 5. Data Integrity

The College undertakes to ensure data integrity by the following methods:

- **Data Accuracy**

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the College of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the College will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

- **Data Adequacy and Relevance**

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the College will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

- **Length of Time**

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Principal to ensure that obsolete data are properly erased.

## 6. Subject Access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the College's policy is that:

- requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

## **7. Processing Subject Access Requests**

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form, available from the College Office. Completed forms should be submitted to the Principal. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 College dates in accordance with the current Education (Pupil Information) Regulations.

## **8. Authorised Disclosures**

The College will, in general, only disclose data about individuals with their consent. However there are circumstances under which the College's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- pupil data disclosed to authorised recipients related to education and administration necessary for the College to perform its statutory duties and obligations.
- pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the College.
- staff data disclosed to relevant authorities eg in respect of payroll and administrative matters
- unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the College. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.
- only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the College by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the College who need to know the information in order to do their work. The College will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A “legal disclosure” is the release of personal information from the computer to someone who requires the information to do his or her job within or for the College, provided that the purpose of that information has been registered.

An “illegal disclosure” is the release of information to someone who does not need it, or has no right to it, or one which falls outside the College’s registered purposes.

## **9. Data and Computer Security**

Frome College undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

- **Physical Security**

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the College are required to sign in and out, to wear identification badges whilst in the College and are, where appropriate, accompanied.

- **Logical Security**

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (ie security copies are taken) regularly.

- **Procedural Security**

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Governors’ Business Committee and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The College’s security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the College should in the first instance be referred to the Principal.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from The Business Manager.

## ACCESS TO PERSONAL DATA REQUEST

### DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname .....

Enquirer's Forename/s .....

Enquirer's Address .....

.....

.....

.....

Enquirer's Postcode .....

Telephone Number .....

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?

YES / NO

If NO,

Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?

YES / NO

If YES,

Name of child, or children, about whose personal data records you are enquiring

.....

.....

.....

.....

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Additional information:

Please despatch Reply to: (if different from enquirer's details as stated on this form)

Name: .....

Address: .....

.....

.....

Postcode: .....

## DATA SUBJECT DECLARATION

I request that the College search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the College.

I agree that the reply period will commence when I have supplied sufficient information to enable the College to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

.....

Name of "Data Subject" (or Subject's Parent)

(PRINTED).....

Dated .....