



**Bearwood College**

Wokingham

Berkshire RG41 5BG

Tel: 0118 974 8300 Fax: 0118 977 3186

# DATA PROTECTION POLICY

Bearwood College is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, pupils and visitors to share this commitment.

All outcomes generated by this document must take account of and contribute to safeguarding and promoting the welfare of children and young people at Bearwood College.

The Bearwood College Policy Documents are revised and published periodically in good faith. They are inevitably subject to permanent revision. On occasions a significant revision, although promulgated within College separately, may have to take effect between the re-publication of the entire set of Policy Documents. Care should therefore be taken to ensure, by consultation with the Senior Management Team, that the details of any Policy Document are still effectively current at a particular moment.

While this current Policy / Procedure may be referred to elsewhere in Bearwood College documentation including particulars of employment, it is non-contractual.

Authorised by the Headmaster on behalf of the Governors, following Resolution by the Board in January 2012

# DATA PROTECTION POLICY

## General Statement

The Board of Governors of the College has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headmaster and Governors of the College aim to comply with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware through this Policy of their duties and responsibilities within these guidelines.

## Enquiries

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

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Telephone: 01625 545 700  
Email: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)

## Fair Obtaining and Processing

Bearwood 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.

## **Registered Purposes**

The Data Protection Registration entries for the College are available for inspection, by appointment, at the Bursar’s Office. Explanation of any codes and categories entered is available from the Bursar 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.

## **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 on request 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, the College will try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Chairman of Governors for his judgement. 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, from time to time the Bursar will monitor records 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 Bursar to ensure that obsolete data is properly erased.

## **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 scholar, the College's policy is that:

- ◆ Requests from scholars 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 scholar does not understand the nature of the request.
- ◆ Requests from scholars 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.

## **EYFS**

At EYFS level, parents have free access to their child's EYFS Profile. However a written request must be made for personal files.

## **Academic References**

The College will not provide scholars or parents with copies of academic references supplied to other academic institutions where the College has a duty of confidentiality to the original recipient.

## **Violent Warning Markers**

The College does not currently utilise "violent warning markers" in its data.

## **Processing Subject Access Requests**

Requests for access must be made in writing.

Scholars, parents or staff may ask for a Data Subject Access form available from the Bursar. Completed forms should be submitted to the Bursar. 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 (e.g. Scholar 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 days (excluding Saturdays) in accordance with the current Education (Pupil Information) Regulations.

### **Charges**

The College charges £40 for each subject Access Request in order to cover staff costs, photocopying and administration.

### **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:

- ◆ Scholar data disclosed to authorised recipients related to education and administration necessary for the College to perform its statutory duties and obligations.
- ◆ Scholar data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- ◆ Scholar 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.

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 scholars' 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.

## **Data and Computer Security**

Bearwood 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. 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.

### **Login Security**

Username and password logins are required on all computers containing personal data. Only authorised users are allowed access to the computer files. 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 pre-employment 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.

### **Destruction of Data**

In accordance with the timing indicated by the College's “Preservation of Records Policy”, staff must destroy all data, including all printed or written records, carefully using appropriate means. The most common means of doing this is by using the shredder located in the Photocopying Room.

The College may respond positively to requests for personal information received from organisations exercising a crime prevention or law enforcement function (e.g. the Police, Social Services etc). The Headmaster (or in his absence a member of the Senior Management Team exercising delegated responsibility) is responsible for any such decision, the details of which are appropriately recorded.

Overall security policy for data is determined by the Headmaster and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

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

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 a serious breach could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from the Bursar.

Bearwood College is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, pupils and visitors to share this commitment.

All outcomes generated by this document must take account of and contribute to safeguarding and promoting the welfare of children and young people at Bearwood College.

The Bearwood College Policy Documents are revised and published in good faith. They are inevitably subject to permanent revision. On occasions a significant revision, although promulgated within College separately, may have to take effect between the re-publication of the entire set of Policy Documents. Care should therefore be taken to ensure, by consultation with the Senior Management Team, that the details of any Policy Document are still effectively current at a particular moment.

While this current Policy / Procedure may be referred to elsewhere in Bearwood College documentation, including particulars of employment, it is non-contractual.

## DATA PROTECTION AND SIMS

### Staff Guidelines

Under the Data Protection Act 1988 the electronic data policy and organized paper filing systems used by the College are controlled. Under the terms of the act the Data Controllers are the Governors and Headmaster. However, in practice, they delegate the role to appropriate individuals such as the following:-

HMM's	Pastoral Data
HOD's	Academic Achievement Data
Registrar	Admissions
College Secretary	Scholar Data
Headmaster's Administrator	Academic Staff Data
Bursar	Support Staff Data

You therefore need to be aware that the Data Protection Act requires the following of them:-

1. to process data fairly and lawfully
2. to obtain specific data for lawful purposes and not to process it in any manner incompatible with that purpose including giving it to a third party or sending it abroad
3. to maintain accurate data and keeping it up to date
4. to prevent the processing of any data likely to cause distress
5. to take appropriate technical and organizational measures to prevent unauthorised access or unlawful processing of the data or against accidental loss, destruction or damage of personal data

Particular regard must be had to the threat posed to data through:

1. leaving computers turned on and logged in to SIMS. Were unlawful access to be gained to the data of personnel through this means then the relevant member(s) of staff and the College as a whole may be liable to investigation by the Data Protection Registrar if a complaint was made by a scholar or parent.
2. not destroying media and printed data carefully. All printed data and/or electronic media must be destroyed in accordance with the timing indicated by the College's "Preservation of Records Policy" carefully and fully using at least a shredder.

Data must be protected by adhering to the following directions:-

<b>DATA PROTECTION: STAFF PROCEDURE DIRECTIONS</b>	
<b>1.</b>	<b>Your login to the network and SIMS must be kept confidential. DO NOT give this to anyone else to use. Always log off SIMS when you have finished using it.</b>
<b>2.</b>	<b>Always log off your computer if you will be significantly away from it and it remains accessible to others; the use of a timed password-protected screensaver is recommended.</b>
<b>3.</b>	<b>Turn off your computer if you are away from it for a substantial period of time.</b>
<b>4.</b>	<b>Never leave your office or classroom unlocked if that means equipment, possessions or sensitive information being left vulnerable.</b>
<b>5.</b>	<b>Do not share any of the information held by the College with anyone who has not been given direct access to it in their own right.</b>
<b>6.</b>	<b>Any sensitive printouts or files must be kept as confidential. Computer files should be in your H: drive; paper files should be in a folder, preferably punched and bound and kept locked; sensitive information should be shredded after use.</b>
<b>7.</b>	<b>If you are unsure about the use of SIMS or how to do something within SIMS, you must contact the ICT Manager or College Secretary.</b>
<b>8.</b>	<b>If you are using SIMS you must ensure that scholars cannot see any sensitive information on the screen.</b>

- 9. All printed data must be destroyed in accordance with the timing indicated by the College's "Preservation of Records Policy" by shredding and all electronic media must be destroyed by shredding or more specialist means.**

**This is not by any means an exhaustive summary of the implications of the Data Protection Act and you should speak to the Data Controller (Headmaster) or the Bursar if you have any additional questions.**



## ADMINISTRATIVE INSTRUCTION

### SECURING COMPUTERS

When you leave a computer switched on you potentially breach the Data Protection Act that requires you to ensure that Data is secure. [NB if you leave your office unlocked this situation is exacerbated as paper systems also need securing].

If your computer is being left you should ensure that unauthorized personnel do not access sensitive data by **Locking** your screen as follows:

1. **Step 1:** Press **Ctrl + Alt + Delete**. The following screen appears:



2. **Step 2:** Select **Lock Computer**
3. **Step 3:** On your return to the office press **Ctrl + Alt + Delete** to access the **Unlock Computer** screen (below) and enter your password in the normal way.



**ACCESS TO PERSONAL DATA REQUEST  
(DATA PROTECTION ACT 1998 Section 7)**

Enquirer's Surname		
Enquirer's Forenames		
Enquirer's Address		
Enquirer's Postcode		
Telephone Number		
Are you the person (i.e. the "Data Subject") who is the subject of the records you are enquiring about?	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.		
Signature of "Data Subject" (or Subject's Parent)		
Name of "Data Subject" (or Subject's Parent) (PRINTED)		
Dated		

**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).



## **SUBJECT ACCESS LOG BOOK**

<b>Date of Receipt</b>	<b>Data Subject's Name</b>	<b>Name And Address Of Requester</b>	<b>The Type Of Data Required (e.g. student record, personnel record)</b>	<b>The Planned Date of Supplying the Information (normally not more than 40 days from the request date)</b>	<b>Information Required, I.E. 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</b>