POLICY/PROCEDURE

Bexhill College

DATA PROTECTION POLICY

POLICY NUMBER: PG7

Reviewed & Approved by Personnel Committee: **JUNE 2010**
Reviewed & Approved by Corporation: **JULY 2010**

REVIEWED: JUNE 2010

DATA PROTECTION POLICY

INTRODUCTION

Bexhill College is registered under the Data Protection Act and needs to keep certain information about its employees for reference purposes and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid.

The College must comply with the Data Protection Principles that are set out in the Data Protection Act 1998. In summary these state that personal data will:

1. Be obtained and processed fairly and lawfully and will not be processed unless certain conditions are met.

2. Be obtained for a specified and lawful purpose and will not be processed in any manner incompatible with that purpose.

3. Be adequate, relevant and not excessive for those purposes.

4. Be accurate and kept up to date.

5. Not be kept for longer than is necessary for that purpose.

6. Be processed in accordance with the data subject's rights.

7. Be kept safe from unauthorised access, accidental loss or destruction.

8. Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Rights for Individuals under the Data Protection Act 1998:

- Right of subject access (to data held on computer records and relevant filing systems upon making a request in writing and paying a fee).
- Right to prevent processing likely to cause unwarranted and substantial damage or distress.
- Right to prevent processing for the purposes of direct marketing.
- Right to compensation.
- Right to correction, blocking, erasure or destruction.
- Right to ask the Information Commissioner to assess whether the DPA has been contravened.

Criminals Offences under the Data Protection Act 1998:

- Processing without notification.
- Failure to comply with an enforcement notice.
- Unlawful obtaining or disclosure of personal data.
- Selling or offering to sell personal data without the consent of the data subject.

Bexhill College and all staff who process or use any personal information should ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy.

We regard the lawful and correct treatment of personal information by the College as very important to the way we work and for maintaining confidence between ourselves and those with whom we deal. We therefore make every effort to ensure that personal information is treated lawfully and correctly.

STATUS OF THE POLICY

This Policy does not form part of the formal contract of employment, but it is a condition of employment that employees abide by the rules and policies made by the College from time to time.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated Data Controller initially. If the matter is not resolved it should be raised as a formal grievance.

NOTIFICATION OF DATA HELD AND PROCESSED

All staff, students and other users are entitled to:

- Know what information the College holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the College is doing to comply with its obligations under the 1998 Act.

Bexhill College has made a standard form of notification available to all staff and students. This states all the types of data the College holds and processes about them, and the reasons for which it is processed.

COMPLIANCE FRAMEWORK

The College, as a body corporate, is the Data Controller under the Act and the Corporation is therefore ultimately responsible for implementation.

The designated Data Controllers on behalf of the College are:

- Personnel Manager
- Student Support Manager
- MIS Manager

The Data Controllers are responsible for data within their management responsibility within the College.

The Data Protection Officer on behalf of the College is the Personnel Manager.

The Data Protection Team will be responsible for:

- Data Protection Policy
- The Data Protection Notification
- Review of Procedures
- Data Protection Audits

REVIEWED: JUNE 2010

A copy of the Data Protection Policy will be held on Blackboard. A full paper copy will be held by Personnel Manager, the Student Support Manager and in the Staff Handbook.

RESPONSIBILITIES OF STAFF

As a member of staff you are responsible for:

- Checking that any information you provide to the College in connection with your employment is accurate and up to date.
- Informing the College of any changes to information which you have provided, e.g. changes of address.
- Checking the information that the College will send out from time to time, giving details of information kept and processed about you.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless you have informed the College of them.

If, and when, as part of your responsibilities, you collect information about other people, e.g. students (opinions on reports; references; marks; details of personal circumstances) you should follow the guidelines for staff.

STUDENT OBLIGATIONS

Students must ensure that all personal data provided to the College is accurate and up-to-date. They must ensure that changes of address, etc. are notified to their Personal Tutor.

Students who use the College computer facilities may, from time to time, process personal data. If they do they must notify the College's Data Protection Officer. Any student who requires further clarification about this should contact the Data Protection Officer.

DATA SECURITY

As a member of staff you are responsible for ensuring that:

- Any personal data that you hold is kept securely.
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.
- Any unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be:

- Kept in a locked filing cabinet.
- In a locked drawer.
- If it is computerised, be password protected.
- Kept only on disk which is itself kept securely.

RIGHTS TO ACCESS INFORMATION

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Anyone who wishes to exercise this right should complete the College "Access to Information" form and give it to the Personnel Manager for staff and Student Support Manager for students.

The data subject must supply sufficient information to enable the College to locate the information that the subject seeks. The College is not obliged to comply with open-ended requests. The College may refuse to disclose data that makes reference to the personal data of third parties.

The College may make a charge of £10.00 on each occasion that access is requested. A register of requests will be kept.

The College aims to provide access to personal information as quickly as possible, but will make sure that it is provided within 40 calendar days unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing to the person making the request.

DISCLOSURE OF PERSONAL DATA

Disclosure of data to authorised recipients takes place as part of the day-to-day business of the College. Authorised disclosure will take place according to the schedule in the College's Data Protection Act Notification.

Personal data must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Particular discretion must be used before deciding to transmit personal data by fax or email.

Where non-routine requests are made or where staff are unsure of their responsibilities they should seek the advice of their Line Manager. The Line Manager may decide to refer a request for a definitive decision to the Data Controller or to the Data Protection Officer. The Data Protection Officer will provide advice about the interpretation of the Act.

Staff should be aware that those seeking information about individuals may use deception to obtain information. Staff should take steps to verify the identity of those seeking information, for example by obtaining the telephone number and returning the call or by reviewing identification documents if and application is made in person. All applications for data should be made in writing.

Requests by other public bodies, including the police, must meet the requirements for lawful processing. The police must be able to demonstrate that they require the information in pursuit of a criminal investigation.

Where a disclosure is requested in an emergency, staff should make a careful decision as to whether to disclose, taking into account the nature of the information being requested and the likely impact on the subject of not providing it.

PUBLICATION OF BEXHILL COLLEGE INFORMATION

Information that is already in the public domain is exempt from the 1998 Act. It is Bexhill College policy to make as much information public as possible.

The Freedom of Information Act also gives the right to ask any public body for all the information they have on any chosen subject. And unless there's a good reason, they have to provide the information within a month. In order to comply with this act the College has a Freedom of Information Publication Scheme available from the Clerk to the Corporation or on the College's website.

This scheme describes the information that the College intends to publish. However, in addition to this, certain personal data will be available to the public for inspection:

- Names of College Governors.
- Register of interests of Governing Body members and senior staff with significant financial responsibilities (for inspection during office hours only).
- Lists of Staff.

The College internal phone list will not be a public document.

Any individual who has good reason for wishing details in these lists or categories to remain confidential, should contact the Personnel Manager.

SUBJECT CONSENT

In many cases, Bexhill College can only process personal data with the consent of the individual.

Agreement to Bexhill College processing certain types of personal data is a condition of employment for staff. This includes information about previous criminal convictions.

All employees of Bexhill College will come into contact with young people between the ages of 16 and 18 and will be subject to CRB checks. Bexhill College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job. We also have a duty of care to all staff and students, and must, therefore, make sure that employees and those who use Bexhill College facilities do not pose a threat or danger to other users.

Bexhill College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. We will only use the information in the protection of the health and safety of the individual, but will need **consent to process** in case of a medical emergency, for example. Consequently, all prospective staff and students will be asked to sign a consent agreement, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form could result in the offer being withdrawn.

EXAMINATION RESULTS

Students will be entitled to information about their performance for both coursework and examinations. Examination results are normally notified directly to students. Lists of examination results identifying individual students are not posted on College notice boards. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or books and equipment returned to the College.

Examination results are made available to the Local Authority (LA) and Heads of partner schools.

Examination results may be made available for publication in the local newspapers. The College does not have to obtain specific consent to publish results but students have a right to object to publication. News stories focusing on individual students will only be made available with the consent of the student.

PROCESSING SENSITIVE INFORMATION

When data is sensitive, **express consent** must be obtained to share the information with other specified individuals. Sometimes it is necessary to process information about a person's health, criminal convictions, race, ethnicity, gender, and family details. This may be to ensure Bexhill College is a safe place for everyone, or to operate other Bexhill College policies, such as the sick pay policy or equality and diversity policy. Because this information is sensitive and we recognise that the processing of it may cause concern or distress, staff and students will be asked to give express consent for Bexhill College to do this. In some cases offers of employment may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Personnel Manager.

TELECOMMUNICATIONS, CCTV AND IT INFRASTRUCTURE

Computer accounts are the property of the College and are designed to assist in the performance of the work of employees and students. There should, therefore, be no expectation of privacy in any stored work or messages sent or received, whether of a business or of a personal nature.

When sending emails on the College's system, the sender is consenting to the processing of any personal data contained in that email and is explicitly consenting to the processing of any sensitive personal data contained in that email. If individuals do not wish the College to process such data, they should communicate it by other means.

The College has the right to monitor any and all aspects of its telephone and computer systems, and to monitor, intercept and/or record any communications made or received by employees, including telephones, email or Internet communications.

Employees and students should be aware that Close Circuit Television (CCTV) is in operation for their protection and the security of College property.

Further information is available in the College's Acceptable Use of Computers Policy.

THE DATA CONTROLLER AND THE DESIGNATED DATA CONTROLLER(S)

The College, as a body corporate, is the Data Controller under the Act, and the Corporation is therefore ultimately responsible for its implementation. However the Personnel Manager is the College's Data Protection Officer and deals with day-to-day matters and is therefore the first point of contact for enquirers. The Personnel Manager will co-ordinate requests for information for both staff and students and they are supported by an Assistant Data Controller.

REFERENCES

The provision of a reference will generally involve the disclosure of personal data. The College is responsible for references given in a corporate capacity. All staff references requested should be referred to the Personnel Manager. All references provided in a corporate capacity about employees and students will incorporate a standard disclaimer paragraph agreed by the College.

The College is not responsible for references given in a personal capacity. These should never be provided on College stationery and should be clearly marked as personnel.

The College will not provide subject access rights to confidential references written on behalf of the College about employees and students and sent to other organisations. This is a specific exemption allowed by the Act.

The College recognises that once the reference is with the organisation to whom it was sent then no specific exemption from subject right access exists.

The College will normally provide subject right access to confidential references received about employees and students provided to the College by other organisations. However the College may withhold information if it is likely to result in harm to the author or some other person of it reveals information about another third party other than the previous supervisor or manager of the employee.

RETENTION OF DATA

The College will keep some forms of information for longer than others. Due to storage restrictions, information about students cannot be kept indefinitely, unless there are specific requests to do so. A list of the archiving retention times employed by the College is included as Appendix 1.

DISPOSAL OF DATA

Particular care must be taken with the disposal of personal data. Staff should be aware that the same standards should be applied to informal records, lists and printouts held by individual members of staff containing personal data as to records, which are part of the formal College records systems.

This material must not be disposed of in ordinary office waste paper bins.

Personal data must be destroyed by secure methods such as shredding or confidential waste sacks handled by authorised contractors.

Formal records may only be destroyed with the appropriate authority.

CONCLUSION

It is the legal responsibility of all members of Bexhill College to ensure that they fulfil their role at the College within the terms of the 1998 Act. This policy lays out the College's obligations to you under the Act and your obligations to students and other members of staff. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken or even to a criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Personnel Manager.

APPENDIX 1 – RETENTION OF RECORDS CONTAINING PERSONAL DATA

The Office of the Information Commissioner says that it is up to each institution to determine how long they keep data relating to personal information. The AoC and JISC however make the following recommendations:

TYPE OF RECORD	SUGGESTED RETENTION PERIOD	REASON FOR THE LENGTH OF PERIOD
Personnel files including training needs and notes of disciplinary and grievance hearings.	6 years from the end of employment.	References & potential litigation.
Application forms/interview notes.	At least 6 months from the date of the interview.	Time limits on litigation.
Facts relating to redundancies where less than 20 redundancies.	6 years from the date of redundancy.	Time limits on litigation.
Facts relating to Redundancies where more than 20 redundancies.	12 years from the date of redundancy.	Limitation Act 1980.
Income Tax and NI returns, including correspondence with tax office.	At least 3 years after the end of the financial year to which the records relate.	Income Tax (employment) Regulations 1993.
Statutory maternity pay records and calculations.	As above.	Statutory maternity pay (General) Regulations 1982.
Statutory sick pay records and calculations.	As above.	Statutory sick pay (General) Regulations 1982.
Wages and Salaries records.	6 years.	Taxes Management Act 1970 .
Accident books & records and reports of accidents.	3 years after the date of the last entry.	Social Security (Claims & Payments) Regulations 1979; RIDDOR 1985.
Health records.	During employment.	Management of Health & Safety at Work Regulations.
Health records where reason for termination of employment is connected with health, including stress related illness.	3 years.	Limitation period for personal injury claims.
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999.	40 years.	Control of Substances Hazardous to Health Regulations 1999.
Student records including academic achievement and conduct.	At least 6 years from the date the student leaves in case of litigation for negligence.	Limitation period for negligence.
Student records including academic achievement and conduct.	AoC recommends records are kept for personal and academic references for 10 years, with agreement of the student.	
Student records including academic achievement and conduct.	Certain personal data may be held in perpetuity.	While personal and academic records may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to her/him ceases to be personal data.
Coursework.	Exam boards say we must keep course work until the November after the June examination. AS coursework should be kept until the student has completed the A2.	Coursework will be kept until the end of Spring Term following the summer exam series.