POLICY/PROCEDURE

Bexhill 6th Form College

DATA PROTECTION POLICY

POLICY NUMBER: PG7

Reviewed & Approved by Personnel Committee: April 2018

REVIEWED: April 2018

DATA PROTECTION POLICY

Bexhill 6th Form College

INTRODUCTION

Bexhill College is registered under the Data Protection Act and needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, for reference purposes and health and safety, for example. It is also necessary to process information for the effective operation of the College and to meet our legal and statutory obligations in relation to regularity and funding bodies and the government. To comply with the law, information must be collected and used fairly, stored safely and securely and not disclosed to any other person or third party unlawfully. Bexhill College is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

To do this, the College must comply with the Data Protection Principles that are set out in the Data Protection Act 1998 and the General Data Protection Regulations (GDPR) 2018. 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.

Bexhill College and all staff who process or use any personal information should ensure that they follow these principles at all times. Breach of the Act can lead to both criminal and civil liabilities. 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.

EXTENT OF THE POLICY

The Data Protection Policy covers all computerised and manual processing relating to identifiable individuals. It not only includes information about individuals, but also options and intentions towards an individual. It therefore includes, for example, Human Resources

records about staff, student records, e mails relating to identifiable individuals, team meeting minutes, student and staff references.

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 Protection Officer on behalf of the College is the Director of Human Resources. The Director of Human Resources deals with day-to-day matters and is therefore the first point of contact for enquirers. The Director of Human Resources will co-ordinate requests for information.

A copy of the Data Protection Policy is available on the staff portal.

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
- Any personal data that you have is only kept for as long as necessary (see Appendix 1).
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.
- No personal data is transferred to a country or a territory outside of the European Economic Area (EEA).
- Registers and other classroom documents are not disclosed on whiteboards – particularly where bursary, attendance, health issues and other information is held.
- Personal information about students is not taken off site unless agreed by a member of the Senior Leadership Team.
- Any unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

All personal data should be accessible only to those who need to use it. Therefore, personal information should be:

- In a locked office
- Kept in a locked filing cabinet.
- In a locked drawer.
- If it is computerised, be password protected.
- Kept only on a memory stick which is itself kept securely. (The ICT policy provides guidance on storage, transmission, encryption and disposal of data owned by the College).

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 Director of Human Resources for staff and Student Services 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 in line with ICO guidelines for each access request. Data subjects will be informed when a request is received. 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 a calendar month 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.

If the College refuses a data request the data subject will be informed in writing, explaining the reasons for the refusal.

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 20 working days. In order to comply with this act the College has a Freedom of Information Publication Scheme available from the PA to the Principal or on the College's website. Charges will apply and some fees may be applied on an individual request basis depending on the information required.

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 members of the Corporation
- Register of interests of Corporation members and senior staff with significant financial responsibilities (for inspection during office hours only).

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 Director of Human Resources.

SUBJECT CONSENT

Although it is not always necessary to gain consent from individuals before processing their data, the College will issue Privacy Notices to ensure that data is collected and processed in an open and transparent manner.

The College interprets consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (via the enrolment form or contract of employment or other associated documentation), where explicit consent is needed. The College understands consent is being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

In some cases, Bexhill College can only process personal data with the consent of the individual. For example, if the data is sensitive, expressed consent must be obtained.

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 and associated partners e.g host families, agency staff and contractors of Bexhill College will come into contact with young people between the ages of 16 and 18 and will be subject to a DBS check. Bexhill College has a duty under the Childrens Act and other

legislation 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 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).

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

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 Director of Human Resources.

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 for reasons of personal security and safety and to protect the College premises and the property of the College, it's staff and students

Close Circuit Television (CCTV) is in operation. The presence of these cameras may not be obvious.
Further information is available in the College's Acceptable Use of Computers Policy.

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 Director of Human Resources or the Principal.

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 personal.

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 the requesting subject 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 if 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 bins handled by authorised contractors. If a confidential waste bin is full you need to notify the Property Manager immediately and use another bin.

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 and 2018 Acts. 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 Director of Human Resources.

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. These apply to staff, Governors and other volunteers.

TYPE OF RECORD	SUGGESTED RETENTION PERIOD	REASON FOR THE LENGTH OF PERIOD
All staff emails	3 years at that date of the email	
Employees work and emails who have left employment	6 months from the end of employment	Time limits on litigation
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 1 year from the closing date .	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.
Finance Records	6 years from the end of the financial year to which the records relate	Companies Act 2006
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.	At least 3 years after the end of the financial year to which the records relate.	Statutory maternity pay (General) Regulations 1982.
Statutory sick pay records and calculations.	At least 3 years after the end of the financial year to which the records relate.	Statutory sick pay (General) Regulations 1982.
Wages and Salaries records.	6 years from the last date of employment.	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.	6years from the end of employment.	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.	Paper records are retained for 6 years from the date the student leaves in case of litigation for negligence. Electronic records are kept for personal and academic references for 10 years,	Limitation period for negligence. 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.
Complaints	3 years from the last action on a complaint	

TYPE OF RECORD	SUGGESTED RETENTION PERIOD	REASON FOR THE LENGTH OF PERIOD
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.

APPENDIX 2: ADVICE FOR STAFF ON THE 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 Policy.

Personal data must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. In this context, third parties may include family members, friends, local authorities, government bodies, lawyers and the police unless the disclosure is authorised by the individual concerned or exempt under the 1998 act or by other legislation.

The Act however, does permit the release of certain types of data without expressed consent in certain circumstances which are:

For the purpose

- for the purpose of protecting the vital interests of the individual (e.g. release of medical data where failure to do so could result in harm to, or the death of, the individual)
- for the prevention or detection of crime
- for the apprehension or prosecution of offenders
- for the assessment or collection of tax
- where the disclosure is required whether as a statutory requirement or in response to a court order.

Most bodies that may request personal data in such circumstances should be able to provide documentary evidence to support their request. For example, many police forces have a specific procedure for requesting information in support of an ongoing investigation. The absence of such documentation, court order or a warrant may justify refusal to disclose personal data. Requests by other public bodies, including the police, must meet the requirements for lawful processing.

Where there is a statutory obligation to disclose, the disclosure must be made. Requests of this nature should be passed to the Principal for staff and the Vice Principals for students.

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 Principal, Vice Principals or Director of Human Resources who will provide advice about the interpretation of the Act.

The College will make all reasonable efforts to obtain the consent of data subjects, staff and students, where non-sensitive personal data (including photographs) is to be used on the College internet and intranet web pages and in other publications where such use is not for the purposes of the normal organisational functioning and management of the institution, for example general marketing purposes including publicity photographs, press releases, prospectus etc.

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. Telephone disclosure is generally unsatisfactory, as verification of such details (and the identity of the enquirer) can be difficult. For example, a student's address, telephone number or e-mail should not be given to a telephone enquirer, even if the enquirer claims to be a

close relative or friend. If a phone call is received from a third party requesting information on a member of staff or student, information about the individual should not be disclosed, however hard the caller may press, without the express permission of the individual concerned. Offer to attempt to contact the individual concerned and take details of the request for information, including the caller's number. If necessary ask them to put their request in writing and offer to accept a sealed envelope to forward to the individual concerned. Follow similar guidelines when dealing with written requests for information.

All applications for data should be made in writing. Particular care should be taken when disclosing sensitive personal data or information that could potentially cause the student or member of staff to suffer subsequent damage and/or distress.

Please note that even confirming whether or not a student or member of staff studies or works at the College could be a potential breach of the Act.

All data subject access requests should be passed to the Data Protection Officer or a member of Senior Leadership team. Staff should note that it is important that personal data relating to other identifiable individuals mentioned in the documents (e.g. other staff or students) should not also be revealed unless permission for disclosure is given by the individual(s) concerned. Thus, a data subject enquirer has the right to see notes or comments relating to them that are held by the College in manual or electronic form, but the identity of the individual(s) who made those comments would not normally be revealed without their express permission. In such situations, any references to third parties must be redacted.
Student references are the responsibility of the Head of Section and should be passed to your HoS.

All staff references are the responsibility of the Principal and Director of Human Resources and should be passed to HR.

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. At least 3 identifying data checks should be sought i.e. is the caller the students next of kin/emergency contact, a date of birth, full address with postcode.

Personal data should be disposed of when no longer needed for the effective functioning of the College and its members (see Appendix 1 for period of retention for records). The method of disposal should be appropriate to the sensitivity of the data. It is recommended that data on paper be shredded and that electronic data be permanently destroyed by reformatting or overwriting. Note that 'deleting' a computer file does not equate to destroying the data: such data can often be recovered. I.T. Services will provide advice as appropriate. Removable hardware for example CD's, DVD's and portable storage devices, should behanded to IT for secure disposal of the data. Overnight all emails that are more than 3 years old are wiped from the College system. Including those emails saved in files.