

Data Protection Policy



Purpose

The College needs to keep certain information about employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, the College must comply with the Data Protection Principles, which are set out in the Data Protection Act 1998. In summary these state that personal data shall be:

- obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- adequate, relevant and not excessive for those purposes
- accurate and kept up to date
- processed in accordance with the data subject's rights
- kept safe from unauthorised access, accidental loss or destruction.

and shall not be:

- kept for longer than is necessary for that purpose.
- transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

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

Extent of the Policy

The Data Protection Policy covers all computerised and manual data 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, personnel records about staff, student records, emails 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 will abide by the rules and policies made by the College from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

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

Definition of Data

Personal data covers any data relating to a living individual (e.g. name, address, payroll details, examination results). Sensitive data form a subset of personal data that relate to a living person, recording such matters as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health and criminal convictions.

The processing of data takes place whenever it is compiled, stored or otherwise operated upon. Disseminating the examination results of students involves processing data relating to each of them, as does giving and receiving personal references, producing agenda items or minutes for committees at which students are discussed as individuals, etc. Similarly, data about staff and applicants for posts are processed when they are committed to manual or electronic records held within the College.

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.
- how to gain access to it.
- how to keep it up to date.
- what the College is doing to comply with its obligations under the 1998 Act.

The College will update staff data at least annually. Students' data are updated annually through the enrolment process.

DATA PROTECTION ACT 1998 - INFORMATION FOR STUDENTS

The personal information you provide is passed to the Chief Executive of Skills Funding Agency (SFA) and, where required, the Young People's Learning Agency for England ("the YPLA") to enable those organisations to fulfill their statutory obligations, principally under the Apprenticeships, Skills, Children and Learning Act 2009. Both organisations are registered as data controllers with the UK Information Commissioner's Office. The Skills Funding Agency funds adult further education and skills training, including apprenticeships, in England. The YPLA is responsible for arranging the provision of funding for the education and training of young people in England. The Skills Funding Agency processes learner data on behalf of the YPLA. The information you provide may be shared with other organisations for purposes of administration, the provision of career and other guidance and statistical and research purposes, relating to education or training. Other organisations include the Department for Children, Schools and Families, the Department for Business, Innovation and Skills, Local Authorities, Local Secondary Education Providers, Connexions, Higher Education Statistics Agency, Higher Education Funding Council for England, educational institutions and organisations performing research and statistical work on behalf of the Skills Funding Agency, the YPLA, or partners of those organisations. The Skills Funding Agency also administers the learner registration service (LRS), which uses your learner information to create and maintain a unique learner number (ULN).

At no time will your personal information be passed to organisations for marketing or sales purposes.

Responsibilities of Staff

Staff are responsible for

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to information, which they have provided. i.e. changes of address or contact numbers.

- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

If and when, as part of their responsibilities, staff collect information about other people, (eg about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Personal information should be:

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on disk that is itself secure.

In processing personal data staff are expected to:

- understand and adhere to the eight data protection principles set out in the 'purpose' section at the beginning of this policy document
- manage personal data in accordance with the College Data Protection Policy, other relevant policies and procedures and the guide lines at appendix 1

Staff should note that Data Protection compliance is ultimately the responsibility of all College staff. Individuals can be held legally responsible if they disclose personal information to any unauthorised third party. Breaches of data protection rules are considered to be a disciplinary matter, and may be considered gross misconduct in some cases.

Student Obligations

Students must ensure that all personal data provided to the College are accurate and up to date. They must ensure that changes of address, etc are notified to the student administrator as appropriate.

Students who find themselves in a position where they are processing personal data about staff or other students (e.g. as a student representative on a College committee or team or as a member of the Student Council) must ensure that they comply with the College policy and the requirements of the Act.

Rights to Access Information

Subject to a limited number of statutory restrictions Staff, students (past or present)

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. Any person who wishes to exercise this right should complete the college "Access to Information " form and hand it in to Registry, and it will be forwarded to the Data Controller.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached.

The College will make no charge for the first occasion that access is requested, but may make a charge of £10 per each subsequent request at its discretion.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Subject Consent

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactments to ensure that appointed staff are suitable for the job, and students for the courses offered.

The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

The 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. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and students will be asked to sign a Consent To Process form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Data Controller.

The Data Controller and the Designated Data Controller/s

The College is, as a corporate entity the Data Controller under the Act, and the Corporation is therefore ultimately responsible for implementation. However, there is a designated Data Protection Officer dealing with day-to-day matters. The first point of contact for enquirers is the **Data Protection Officer**, who may either deal with the enquiry her/himself or refer it to another designated individual with inquiry related responsibilities.

Public Register of Data Controllers and Notification

The College has a valid notification in the data protection register that relates to processing information. This can be viewed at <http://www.ico.gov.uk/> It is the responsibility of the Data Protection Officer to ensure the registration is checked and updated on a regular basis.

Registration Number: Z5758025

Annual Registration: December

Data Controller: The Blackpool Sixth Form College

Examination Marks

Students will be entitled to information about their marks for both coursework and examinations.

However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the College.

Exemptions

Generally all personal data collected and processed will be subject to the Data Protection Act. However, some exemptions apply e.g.

References - a confidential reference given by the College to a third party regarding, education, employment/training, appointment to a public office, a service being provided by the data subject etc, will remain confidential and is exempt from the requirements of the Act.

References we have received and kept on file are not exempt. We must, however, ensure that the rights of the referee are considered. Information about the individual referee should not be disclosed without explicit consent (anonymising the information is acceptable). The college cannot refuse to disclose confidential references without providing reasons.

Crime and taxation – personal data may have to be disclosed to government departments or the Police. Data will only be released on the basis of properly drawn up requests.

Vital interests – personal data may be released if it is in the vital interests of the individual e.g. a medical emergency.

Under 19 students – the College will normally release information about a student's progress and attendance to parents or guardians of students under 19 years of age on the previous 31st August.

Retention of Data

The College will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. A list is attached of the archiving guidelines and retention times employed by the College.

Disposal of Data

When personal data is no longer required, or has passed its retention date, paper records must be shredded. If there is a significant amount of material which cannot be dealt with by normal shredding machines, this should be disposed of using a reputable disposal contractor.

Computerised records must be permanently deleted; with particular care taken that 'hidden' data cannot be recovered. The IT Helpdesk can advise on permanent deletion of computerised records.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Controller.

Further Guidance

Information Commissioners' website <http://www.ico.gov.uk/>

Appendix 1 – General Guidelines

Linked Policies and Procedures

- [Staff Code of Conduct](#)
- [Disciplinary Policy and Procedures](#)
- [Clear Workspace Policy](#)
- [Acceptable Use of Computers \(Staff\)](#)
- [Acceptable Use of Computers \(Students\)](#)
- [Data Protection Form \(Students\)](#)
- [Disclosure Policy](#)
- [Safeguarding Policy](#)
- [FileMaker Password Policy](#)
- [Security Policy](#)
- [Laptop Protocol Policy](#)

Appendix 1

General Guidelines

1. Storing Personal Data

Personal data must be held securely. In the case of manual data this could be in filing cabinets, locked cupboards or rooms with access restricted to named individuals or categories of individual only. In the case of electronic information, access must be subject to reasonable controls including passwords and restricted access rights. Reasonable steps must be taken to detect and prevent unauthorised access. Regular backups should be taken to ensure that important data cannot be lost.

2. Disclosing Personal Data

Personal data should not generally be disclosed to third parties without the permission of the individual concerned. This covers both intentional disclosure and any disclosure that may happen by accident, for example someone having oversight of a monitor on which data is displayed. In this context, 'third parties' include family members, friends, local authorities, government bodies and the police unless disclosure is exempted by the 1998 Act or by other legislation. Under certain circumstances, data may however be released. Note that among other circumstances the Act permits release of data without express consent:

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

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.

As a rule, personal or sensitive data should not be disclosed without the express consent of the individual concerned. 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.

3. Protecting Third Parties

In meeting a data subject access request, 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.

Where it might be unrealistic to obtain consent, for example if the third party's whereabouts are unknown, a judgement should be taken about how reasonable it is in the circumstances to release the information. It may be necessary for example to edit the information to protect the third party's identity.

4. Disposal of Personal Data

Personal data should be disposed of when no longer needed for the effective functioning of the College and its members (see Appendix 2 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 be handed to IT Services for secure disposal of the data.

5. Applications for Employment and Education

Notes made in the course of interviews constitute individual data and are therefore subject to access under the Act. They should be fair, reasonable and defensible. Interview notes relating to successful applicants may be retained while the individual is a member of the College, and hence be disclosable in response to a data subject request. Interview notes and all personal data relating to unsuccessful applicants will be retained for up to one year in the case of staff and three years (electronic format) and one year (hard copy) for students after it has become clear that the individual will not be appointed or admitted to the College, but not retained for longer than necessary once that period has elapsed.

6. CCTV and similar surveillance equipment

The College employs closed-circuit television as part of its security systems and complies with the Code of Practice on the use of CCTV issued by the Office of the Information Commissioner.

RECORDS RETENTION SCHEDULE

Type of Data	Retention Period	Reason
Personnel files; training records; notes of grievance and disciplinary hearings	6 years from the end of employment	Provision of references and limitation period for litigation
Staff application forms; interview notes	6 months from the date of the interview for those not appointed.	Limitation period for litigation
Wages and salary records	10 years from the last date of employment	Taxes Management Act
Statutory Maternity and Sick Pay records and calculations	6 years after the end of the financial year to which the records relate	SSP and SMP Regulations
Records and reports of accidents	6 years after the date of the last entry	RIDDOR
Health Records	6 year from the end of employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is concerned with health, including stress-related illness	6 year from the end of employment	Limitation period for personal injury claims
Student Records including academic achievements and conduct	6 years from the last day of the course for paper records and 10 years for electronic subset.	Limitation period for negligence
Contracts and contractual information	7 years after completion of the contract	Limitation period for negligence

GLOSSARY OF MAIN TERMS

Data – any information which will be processed and stored. This can be written, taped, photographic or other information.

Personal Data – information about a living person.

Data Subject – the person whom the data is about.

Data Controller – the person or organisation responsible for ensuring that the requirements of the Data Protection Act are complied with.

Data Protection Officer – member of staff designated by the College to ensure compliance with data protection policies and procedures.

Data Processing – accessing, altering, adding to, changing, disclosing or merging any data.

Sensitive Data – information about a person's religion, gender, political beliefs, sexuality, trade union membership, health or criminal record.

Data Protection Principles – the underlying principles that determine what data can be collected, processed and stored.

Relevant Filing System – any filing system (paper based or computerised) which is readily structured so that information about an individual is accessible.

Information Commissioner – officer appointed by the State to administer the provisions of the Data Protection Act.

Notification – the process of informing the Information Commissioner that an organisation or individual will be processing personal data other than for private use.

Subject Consent – before processing personal data the agreement of the individual must be obtained.

Under 19 Student – a student who was under 19 on the previous 31st August.