

# LONGLEY PARK SIXTH FORM COLLEGE

## DATA PROTECTION POLICY

### INTRODUCTION

Longley Park Sixth Form College ("the College") needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, health and safety, for example. It also needs 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 collected and 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;
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- Be adequate, relevant and not excessive for those purposes;
- Be accurate and kept up to date;
- Not be kept for longer than is necessary for that purpose;
- Be processed in accordance with the data subject's rights;
- Be kept safe from unauthorised access, accidental loss or destruction;
- Not be 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 the Data Protection Policy.

### DATA PROTECTION ACT 1998 - INFORMATION FOR STUDENTS

Information you provide to the College will be passed to the Young People's Learning Agency (YPLA), the Skills Funding Agency (SFA) and Sheffield City Council (SCC). The YPLA and the SFA are responsible for funding, planning and encouraging education and training for young people and adults in England. All are registered under the Data Protection Act 1998. Information will also be shared with other organisations for the purpose of administration, careers and other guidance, statistical and research purposes, in line with the College's Data Protection Policy. Other organisations with which we will share information include Aim Higher; the Department for Education; the Department for Business, Innovation and Skills; Connexions; educational institutions and organisations performing research and statistical work on behalf of YPLA and SFA or its partners including IpSOS MORI. The YPLA also administers the Learner Registration Service (LRS) which will use your information to create and maintain a unique learner number (ULN). The YPLA and the SFA are also co-financing organisations and use European Social Funds from the European Union to directly or indirectly part-finance learning activities, helping develop employment by promoting employability, business spirit and equal opportunities, and investing in human resources. Further information about partner organisations and the ULN and what they do, may be found at [Skills Funding Agency](#) or [Young People's Learning Agency](#) and by following the links to data protection.

At no time will your personal information be passed to organisations for marketing or sales purposes. From time to time students are approached to take part in surveys by mail and phone, which are aimed at enabling the YPLA and the SFA and their partners to monitor performance, improve quality and plan future provision. Please let us know on your enrolment form, by ticking the relevant box, if you do not wish to be contacted by YPLA and the SFA or their partners in respect of surveys and research. The YPLA and the SFA value your views on the education or training which you receive, and will use these to help bring about improvements for learners in England. The YPLA and the SFA or their partners may wish to contact you from time to time about courses, or learning opportunities relevant to you. Again, please tick the relevant box on the enrolment form if you do not wish to be contacted about courses or learning opportunities by post.

## **THE DESIGNATED DATA CONTROLLER**

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

The designated data controllers on behalf of the College are:

- Personnel Manager
- College Information Systems Manager

The College has a designated Data Protection Officer who is responsible for:

- Maintaining the College's registration with the Information Commissioner's Office;
- Providing advice, guidance and direction on data protection issues within the College.

## **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 failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff or student, 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.

## **RESPONSIBILITIES OF STAFF & STUDENTS**

All staff and students 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 or errors in information, which they have provided, i.e. changes of address. They must ensure that changes of address, etc are notified to Human Resources (staff) and Student Services (students);

- The College cannot be held responsible for any such errors unless the staff member or student has informed the College of them;
- Students who use the College computer facilities may, from time to time, process personal data. If they do so they must notify the relevant Director of Teaching & Learning through their course teacher or progress tutor.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the Staff Guidelines in Appendix 1.

## **DATA SECURITY**

All staff are responsible for ensuring that:

- Any personal data (including personal images) which is held is kept securely, for example in a locked room, locked filing cabinet or locked drawer;
- If it is computerised, it is password protected and that all passwords are regularly changed;
- Data stored on disks is removed before disposal;
- Papers containing personal information are shredded before disposal;
- Databases are closed and workstations securely locked when leaving the computer;
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

## **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. Any person who wishes to exercise this right should contact Human Resources (staff) or the relevant Director of Teaching & Learning (students).

Any other requests should be made in writing to the Data Protection Officer.

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 to the Data Protection Officer.

The College will make a charge of £10 on each occasion that access is requested, although the College has the discretion to waive this.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 28 days.

## **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 in accordance with the [Rehabilitation of Offenders Act 1974](#) and information about disabilities.

Some jobs or courses will bring applicants into contact with children, including young people between the ages

of 16 and 18. The College has a duty to ensure that 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. Therefore, all prospective staff and students will be asked to consent to their data being processed when an offer of employment or a course place is made. A refusal to sign such a form may result in the offer being withdrawn.

## **PROCESSING SENSITIVE INFORMATION**

Processing means obtaining, recording, holding or carrying out any operation on the information or data. Sensitive personal data is a special category. It may only be processed with the explicit consent of the data subjects. Sensitive personal data, including personal images, consists of information relating to;

- the racial or ethnic origin of the data subject;
- political opinions;
- religious or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- the commission or alleged commission of any offence;
- proceedings for any offence or alleged offence.

Sometimes it is necessary to process information about a person's 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 Equality & Diversity Policy.

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

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.

## **EXAMINATION RESULTS**

Students will be entitled to information about their marks 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 Directors of Education, Sheffield City Council, 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 focussing on individual students will only be made available with the consent of the student.

Students do not have subject access right to examination scripts. However they may claim subject access rights to any comments recorded by the examiner in the margins of scripts.

Subject requests for examination marks or results must be met within forty days of the announcement of the results or 5 months from the date the request is received, whichever is the earlier.

## **RETENTION OF DATA**

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. The College will keep some forms of information for longer than others to meet various contractual requirements. Appendix 2 indicates the length of time that records will be retained.

Data on students, including any information on health, race or disciplinary matters, will be destroyed after 6 years but a skeletal record will be retained to include a full transcript of academic achievements for 10 years.

## **DATA PROTECTION AUDITS**

Audits of computerised and manual record systems should be conducted annually.

## **PERIODIC REVIEW OF DATA PROTECTION POLICY**

The Data Protection Officer should review the Data Protection Policy annually.

## Staff Guidelines

- Members of staff will process personal data on a regular basis. The College will ensure that staff and students give their consent to processing and are notified of the categories of processing, as required by the Act.
- Information about an individual's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is sensitive and can only be collected and processed with their express consent.
- Members of staff have a duty to make sure that they comply with the data protection principles, which are set out in the College's Data Protection Policy. In particular, staff must ensure that records are:
  - Accurate
  - Up to date
  - Fair
  - Kept and disposed of safely and in accordance with the College policy
- Individual members of staff are responsible for ensuring that all data they are holding is kept securely.
- Members of staff must not disclose personal data, unless for normal academic, administrative or pastoral purposes, without authorisation or agreement from the Data Protection Officer, or in line with the College policy.
- The College may need to amend its registration with the Office of the Information Commissioner if data held is additional to normal curriculum requirements before commencing processing of the data. Advice is available from the Data Protection Officer.
- Before processing any personal data, all staff should consider the checklist as set out below.

## Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual or data subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate? Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- Have you notified the Data Protection Officer that you intend to hold the data?
- How long do you need to keep the data for, and what is the mechanism for review/destruction?

## Retention of Data

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	6 months from the date of interviews	Time limits on litigation
Facts relating to redundancies (less than 20)	6 years from the date of redundancies	Time limits on litigation
Facts relating to redundancies (more than 20)	12 years from the date of redundancies	Limitation period for litigation
Income tax and NI returns; correspondence with the 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 1986
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 salary records	6 years from the last date of employment	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health records	During 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	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health	40 years	COSHH 1994
Student records including academic achievements and conduct	6 years from the last day of the course. 10 years with the consent of the student for personal and academic references	Limitation period for negligence