PRIOR PURSGLOVE and STOCKTON SIXTH FORM COLLEGE

Data Protection Policy

Introduction

Prior Pursglove and Stockton Sixth Form College is required to keep certain information about its employees, students and other users for various academic and health and safety reasons, e.g. monitoring performance and achievements. 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 General Data Protection Regulations (GDPR) and the Data Protection Act 2018, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The Act states 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.

All those who process or use any personal information must ensure that they follow these principles at all times.

It is a condition of employment that you abide by the rules and policies made by Prior Pursglove and Stockton Sixth Form College. Any failures to follow this policy either deliberately or by neglect can therefore result in disciplinary proceedings.

If you feel that the policy has not been followed in respect of personal data held about you, you should raise the matter with the Data Protection Officer 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 GDPR and the 2018 Data Protection Act.

Responsibilities of Staff

You are responsible for:

- checking that any information you provide in connection with your employment is accurate and up to date.
- informing the Human Resources Officer) of any changes to information which has been provided e.g. change of address, telephone number, qualifications.
- checking the information that you receive from time to time, giving details of information kept and processed about you.
- informing the Human Resources Officer of any errors or changes. We cannot be held responsible for any errors unless you have informed us of them.
- if and when, as part of your responsibilities, you collect information about other people, (i.e. about student course work, opinions about ability, references to other academic institutions, or details of personal circumstances), you must comply with the guidelines for staff, which are at appendix 1.
- ensuring that any personal data which you hold is kept securely e.g.
    - in a locked filing cabinet; or
    - in a locked drawer; or
    - if it is computerised it must be only accessible using a strong password;
- ensuring that you do not disclose personal information (data breach) either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Informing the Data Protection Officer of any data breach.

Unauthorised disclosures may be a disciplinary matter and may be considered gross misconduct in some cases.

Student Obligations

You must ask students to ensure that all personal data provided to the college is accurate and up to date. Students must notify changes of address etc. at the Reception desk or by emailing MIS Support. Ideally this change in information should be backed up with some sort of documentation.

Students may, from time to time, process personal data. If they do this as part of their course, you must ensure that they know the principles of GDPR and the Data Protection Act.

Rights to Access Information

Staff, students and others 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 make a request either orally or in writing to the Data Protection Officer.

The College will make a charge of £10 on each occasion that access is requested, although this may be waived at the discretion of the Data Protection Officer.

We aim to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing.

Publication of Information

Information that is already in the public domain is exempt from the 2018 Act. It is the College's policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names of governors.
- List of staff names and role in college.
- Photographs of staff and governors.

The internal telephone and e-mail directory is not a public document.

Any person who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Protection Officer.

Consent to Process Data

In many cases we can only process personal data with consent. In some cases, if the data is sensitive, express consent must be obtained. Agreement to 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.

It is necessary to share information, on occasion, without consent in cases covered by the Safeguarding Act. In these cases, we would share information with legal, healthcare, and other educational support providers.

The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the course offered. We must therefore make sure that employees, students and those who use College facilities do not pose a threat or danger to other users.

The College will 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 health and safety 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 Privacy Policy Statement 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 policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and may cause concern or distress, staff and students will be asked to give express consent for us to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent, without good reason.

The Data Controller and the Designated Data Controller/s

The Governing Body is ultimately responsible for ensuring that the College complies with GDPR and the Data Protection Act. The College's SLT and MIS Manager will deal with day to day matters.

Retention of Data

The College will keep personal data only as long as our data retention policy dictates.
Student records – 10 years from date of leaving college
Personnel files – 10 years after employment ceases

Conclusion

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 Assistant Principal - Resources.

Date of Last Approval/Revision	December 2019
Review interval (years)	3 years
Responsible Officer	–Data Protection Officer
Approval/review body (ies)	SLT
Date of next review	December 2022
Public File location	Drive L: / Sharepoint documents folder

APPENDIX 1 TO THE DATA PROTECTION POLICY

Staff Guidelines for Data Protection

1. All staff process data about students on a regular basis, when marking registers, writing reports or references. The College will ensure students give their consent to this sort of processing, and are notified of the categories of processing, as required by GDPR and the 2018 Data Protection Act. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

   (a) general personal details including name and address.
   (b) details about class attendance, course work marks and grades and associated comments.
   (c) notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical and mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent, e.g.: recording information about dietary needs, for religious or health reason prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

3. Everyone has a duty to make sure that they comply with the data protection principles, which are set out in the Data Protection Policy. In particular, you must ensure that records are:
   - accurate,
   - up to date,
   - fair,
   - kept and disposed of safely, and in accordance with College policy.

4. You must be responsible for ensuring that all data is kept securely, and report any Data Breach

5. You must not disclose personal data unless for normal academic or pastoral purposes, without authorisation or agreement from the data subject, Manager or member of the SLT.

6. Before recording and processing any personal data, you should consider the following checklist.

   - 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 student been told that this type of data will be processed?
   - 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?
   - Do you need to report the fact of data collection to your Manager?

Confidential References

- It is a requirement that all those giving references must be satisfied that the worker/Student wishes the reference to be provided. When responding to a request from a worker/Student to see his or her own reference and the reference enables a third party to be identified, make a judgement as to what information it is reasonable to withhold.

Complaints

- Any person can apply to the Data Protection Commissioner for assessment. The commissioner will then contact the organisation and require information, possibly within as little as 7 days.
- The commissioner could then require the organisation to change, destroy or cease processing certain information.

Security of Data

- Files should not be available to anybody who has no right to the data. Staff and Student files should always be in the central files in the administration area or kept in a secure place by the member of staff using them.
- All files on computer should be password protected, which means data can only be accessed by using a strong password through your user account.
- Computer backup files are made daily and stored securely.
- All information held on staff and students must be kept in a secure place.
- Any breach of college policy on this matter may be treated under the disciplinary code.

DATA PROTECTION ACT 2018 – ANALYSIS OF STUDENT DATA KEPT BY PRIOR PURSGLOVE AND STOCKTON SIXTH FORM COLLEGE

Type of Information	How kept	Who by/who has access
Name	Manual – student files and records, administration forms, mark books, registers. Computer database	Staff, Tutors, Teaching and Admin
Address	Manual – student files, registers, admin forms. Computer database	Ditto
Telephone Number	Manual – student files, registers, admin forms. Computer database	Ditto
Date of Birth/Ethnicity	Manual – student files, registers, admin forms. Computer database.	Ditto
Correspondence with parents/carers	Manual – in student files	Staff
References	Manual – student files Computer database	Faculty Managers, Tutors, Admin
Exam Results	Manual – results sheets from exam boards, student files, destination lists, mark books. Computer database	Exams Officer + central file, teachers/Admin
Courses and Course changes	Manual – change of course form. Computer database	Staff
Mark & Test Data Estimated grades/actual grades	Manual – mark books, student files and references. Computer database	Teaching Staff Admin Staff
Special Needs	Manual-administration forms, Special enrolment forms, support services information. Computer database	Faculty Manager(s), Learning Support Manager and Assts, Tutors, Admin
Previous School	Manual – administration forms, mark books. Computer database	Teachers, Admin Staff
Attendance/Absence	Manual – registers, mark books. Computer database	Teaching staff, tutors, Admin
Parent/Carer details	Manual – student files Computer database	Admin, tutors, teachers
Health information	Manual – student files, tutor files, application form, examination 'special circumstances' forms, Computer database	Admin, Tutors, Exams Officer, teachers
Review Sheets	Manual – in student files	Teachers, Tutor, Admin
Careers Information	Manual – student files and records Work Experience information	Work Experience and Careers Co-ordinators, Tutors/Admin
Fines and overdue records	Computerised Library System	Resource Centre staff
Photographs	Digital images and hard copies	Staff, Tutors, Admin, Marketing staff

The following Student information is published by college *

Student Enrolment	Details sent to each individual school where student came from, and with whom we have a data sharing arrangement set up.
Student Achievement	examination results (anonymous) are published in local newspaper in August and sent to students' secondary schools. Individual success stories are shared with local media on agreement with the student.
Photographs	Used in college publicity – prospectuses, adverts, web pages, notice boards, displays

* This information is given to students when they enrol in college and they sign a privacy statement.

DATA PROTECTION ACT 2018 – ANALYSIS OF STAFF DATA KEPT BY PRIOR PURSGLOVE AND STOCKTON SIXTH FORM COLLEGE

Type of Information	How kept	Who by/who has access
Staff Files	Manual – application forms, previous posts, qualifications, references and reports. Computer database: names, addresses, date of birth, gender, ethnicity, car registrations, qualifications	Management, Admin staff
Governor Details	Manual – names, addresses, workplace details, Governor service details. Computer – list of names/addresses	Clerk to the Governors, Admin
Personnel and Payroll Information	Manual – Payroll information. Computer database.	Principal, Director of Resources, Chief Finance Officer, Human Resources staff, Finance Staff, Payroll Bureau
Attendance Rates	Manual – reasons for absence Computer database	SLT, Faculty Managers, HR Staff
Staff Development Records	Manual – Reviews Computer database	Vice Principal, HR Staff, Reviewer, Admin

Information kept on Central Computer Database:

- Accessible only by passwords.

Information kept manually:

- Student and Staff files kept in filing cabinets/cupboards in administration area – locked each evening.
- Information kept by teaching staff, eg, mark books, kept in filing cabinets in teaching/tutor rooms, or in members of staff's room. Confidential information kept locked in filing cabinet or briefcase.
- Examinations information kept in locked filing cabinets in Examinations Office.
- Special Needs information kept in locked filing cabinet or carried personally by Learning Support Manager or Learning Support Assistants.
- Personnel and Payroll information kept in locked filing cabinets.
- Information on students who have left kept for 10 years and then shredded.
- Careers & Works Experience Co-ordinators' offices are locked when he/she is off premises.
- No personal information given by telephone to third parties without permission.