

APPENDIX E: HANDLING STUDENT PERSONAL DATA

Introduction

1. The Data Protection Act 1998 governs access to information about individuals held by the College.
2. The Data Protection Act is concerned with personal information about an individual – for example, name, address and date of birth – and lays down sensible rules for the handling of personal data. The Act also confers rights on any individual about whom personal information is processed or held. The Freedom of Information Act provides a general right of access – subject to certain prescribed exemptions – to all information such as policies and procedures, committee minutes and papers held by the College.
3. All members of staff who handle personal information, in this case specifically student information, must not only comply with the Data Protection Act 1998 but are expected to understand that the need for confidentiality extends far beyond its requirements, particularly where sensitive personal information is concerned.
4. This policy has been developed to support the College's Data Protection policy and its commitment to protecting the privacy and confidentiality of all student data as far as is reasonably practicable.

Summary

Collection and management of student data

5. Personal information about students is collected by the College for a number of purposes, both internal to the College and for external education-related agencies.
6. Staff have a duty to ensure that the only information collected suits the stated purpose, is factual, and is kept securely and destroyed in line with College and statutory regulations.

Disclosure of student information under the Data Protection Act

7. Student information should not be disclosed to anyone without proper authority. Where disclosure is requested by someone external to the College, staff should neither confirm nor deny that the person being asked about is a student here.
8. Staff should contact the Data Protection Officer if they have any questions regarding disclosure of student information.
9. Students have a right to know what information the College holds about them, for what purpose(s), and to whom such information might be disclosed. However, the student does not have an automatic right to see all the information.
10. All such requests should be forwarded to the Data Protection Officer for action.

Related policies and further guidance

11. A list of College policies and other documents affecting confidentiality of student information is provided in the Student Contract.
12. The attached appendices give more detailed guidance regarding disclosure to particular people or groups, and disclosure by those services within the College that are bound by a professional code of ethics.

Collection and management of student data

Collection of data

13. Information about the College's students is obtained from UCAS and other admissions clearing houses, from the College application and enrolment forms, and

from individual students themselves. The information that the College collects enables it to manage an individual student's academic career from admission to graduation, through to alumnus, and then to confirm qualifications in the future.

Purposes for which data are held

14. The College needs to hold personal information about students for various teaching, research and administrative purposes in order to administer their academic career, including:
 - (a) maintenance of the student record (including personal and academic details) and management of academic processes (for example, academic audits, examination boards and awarding of degrees);
 - (b) management of accommodation;
 - (c) alumni operations, including fund-raising;
 - (d) provision of advice and support to students via, among others, Registry, personal tutors, Counselling Service, Disability/Dyslexia Service and Placement and Careers Centre;
 - (e) access to facilities such as the Library and computing;
 - (f) internal research, including monitoring quality and performance; and
 - (g) security and car parking.
15. Student information is held in a number of different formats (e.g., on the SITS student database, College/departmental files) and various locations.
16. In addition, the College has a statutory obligation to disclose personal information about students to the Higher Education Funding Council (HEFCE) and the Higher Education Statistics Agency (HESA), which is then passed to relevant government agencies that require the information to carry out their statutory functions regarding the funding of education.

Duties of staff

17. All members of staff who have access to student data as part of their job should at all times ensure that:
 - (a) data is only used for the purpose(s) for which it was collected;
 - (b) data confidentiality is maintained at all times;
 - (c) data accuracy is maintained;
 - (d) data is held securely;
 - (e) only data that is necessary for the conduct of normal College business are retained;
 - (f) confidential data, whether held in paper format or electronically, is securely destroyed when no longer required.
18. In addition, all staff should be aware of a student's right to privacy in matters relating to his/her health and welfare. When advising students, staff should make clear at the outset of a discussion whether the content is to remain confidential and the extent of the confidentiality to be given to any disclosures.
19. In particular, staff should inform the student of the:
 - (a) College's concern to respect privacy, wherever possible;
 - (b) circumstances, if any, under which information may be shared with a third party, taking account of the duty of care that may be owed to the individual or others; and
 - (c) individual or College Departments or other agency that may be informed in such circumstances.

20. All staff should also inform a student, at the outset, of any limits to their impartiality imposed by their responsibility as a College employee.

NOTE: The Human Rights Act 1998, Article 8, states, "Everyone has the right to respect for private and family life, his home and his correspondence."

21. Any staff member who discloses student personal data without proper authorisation may be subject to disciplinary proceedings.

Information to be recorded

22. The contents of all student files, whether paper or electronic files, should be limited to documents that reflect normal College business and that have either been copied to the student or could be copied without causing any distress.
23. All information recorded should be factual. Judgements, comments or opinions should not be included unless information exists to support those judgements or opinions.

Sensitive personal data

24. Certain types of information are considered to be sensitive in nature. These include:
- (a) racial or ethnic origin;
 - (b) political opinions;
 - (c) religious beliefs;
 - (d) membership in a trade union;
 - (e) physical or mental health or condition;
 - (f) sexual life;
 - (g) commission or alleged commission of a criminal offence;
 - (h) proceedings, disposal of proceedings, or results of proceedings against a person for a criminal offence.
25. Some of this data is collected for use in statistical analyses, particularly by the Higher Education Statistics Agency (HESA). However, for this purpose, the data is used anonymously – there is no connection with a particular person.

Security of data

26. Personal student data should be stored securely whether staff work in a private or open-plan office, in line with the College's Data Protection Policy.
27. All staff should ensure that personal data are:
- (a) kept in a locked filing cabinet, drawer, cupboard or room, whether it is in paper or electronic format (e.g., CD, memory stick, etc.) when not being worked on or when the office is left unattended (even for a short time);
 - (b) not visible, either on desks or on computer screens, to any visitors; ensure screen savers and computer screen locks are used. Passwords should not be disclosed to anyone (including managers);
 - (c) sent in a sealed envelope, if transmitted through the internal mail;
 - (d) not sent via email, if it is sensitive information;
 - (e) not disclosed orally or in writing without the permission of the student unless it is part of a legitimate College process;
 - (f) not left on shared printers/ photocopiers;
 - (g) disposed of securely in line with the Retention and Disposal policy whether in paper format or electronically.

Retention and disposal of information

28. All student files should be retained in line with the Records Retention and Disposal Schedules available on the intranet and to students on the regulations and policies website.
29. The majority of student data will be destroyed or deleted seven (7) years after graduation. However, some student personal information will be retained indefinitely as part of the College's history so that at a later date, the College can provide proof of a student's achievement. Such information, however, should only be disclosed with the student's consent unless exceptional circumstances apply.

Disclosure of student information under the Data Protection Act

30. If you receive any request for student information that is out of the ordinary, you should pass the request to the Data Protection Officer for action.
31. You must not disclose sensitive personal data without the student's express consent or without proper authorisation.

Internal disclosure

32. Personal information should only be disclosed to other members of College staff if you have the student's permission or if the disclosure is necessary for the College's legitimate interests. Personal information must not be disclosed merely for social reasons.
33. If you do not know the member of staff who is requesting the information, ask them to produce their ID card or check with the Human Resources Department (HR).

External disclosure

34. Information must not be given out externally, except where there is a legal or contractual requirement to do so, without the student's permission. This includes supplying information to parents, legal guardians and next of kin.
35. If you receive a request via the telephone, you should neither confirm nor deny that the person being asked about is a student at the College. Ask the caller to put the request in writing. Detailed guidance on how to deal with external disclosures can be found below.
36. If confidential information is to be released without the student's permission, the permission of the Senior Officer or Information Asset Owner responsible for the security of that information must be obtained. The student must be informed, except in cases where the College decides this is legally inadvisable.
37. If staff are asked to disclose sensitive personal information regarding, for instance, a student's health or criminal convictions, and they do not have the student's permission, they should confine their statement to something like, "I'm sorry, but I am not in a position to comment." In certain cases, it may be necessary for approval to be granted from the Secretary to Board of Directors or the Chief Operating Officer or their designated agents before information is released.

Subject access requests under the Data Protection Act

38. Under the Data Protection Act 1998, every student has the right to be told whether the College holds personal information about them, to be given a description of those data, the purposes for which they are held and to whom they may be disclosed.
39. To obtain access to personal data the College may hold, students must submit a subject access request, specifying which data they would like to have access to, with

- proof of identification and the appropriate fee to the Data Protection Officer (Governance, Information & Legal Office).
40. The Data Protection Officer is responsible for contacting relevant areas within the College and ensuring that the information requested is/can be released to the student. This must be completed within forty (40) days of receiving the request, the fee and sufficient information to find the data requested.
41. The only types of documents that a student making a subject access request does not have an automatic right to see, which may be kept on a student's file, are:
- (a) references supplied in confidence, which will only be released if the referee has given consent;
 - (b) examination scripts – any information recorded by a student on an examination script is exempt from a subject access request; however, any comments made by a marker whether or not they are on the script must be disclosed if a subject access request is made. Therefore, it is recommended that any comments or opinions are constructive and can be backed up if a subject access request is made. Please note: students are entitled to have their marks if they submit a subject access request even if they are in debt to the College, although they will not be given their official certificates/transcripts and will not be allowed to attend their graduation ceremony;
 - (c) document(s) that identify another individual(s).

Related policies and further guidance

42. Further information can also be found in the following College documents:
- (a) Data Protection policy.
 - (b) Records Management policy.
 - (c) Records Retention and Disposal policy and schedules.
 - (d) CCTV policy.

Guidance on external disclosures

Parents/spouses/other relatives

- Students' family members do not have a general right to information about their child, partner etc., though they often assume they do.
- Information can only be provided if the student has given their permission.
- If someone claiming to be a parent, spouse, partner etc. contacts the College wanting information, staff should take their details, contact the student and ask them to contact the individual directly.
- Do not confirm or deny that the person the caller is asking about is a student.

Sponsors

- Sponsors and similar bodies (e.g., LEAs, Embassies, High Commissions, private companies, charities, etc.) do not have a general right to information about the personal data of 'their' students, although the College may provide academic information.
- If you receive a request from a sponsor, ask them to submit their request in writing. If, on receiving the request, you are unsure whether to release the information, contact your Head of Department or Data Protection Officer.

Departments

- Students' former schools/colleges do not have a right to information about their former pupils.
- Information can only be provided if the student has given their permission.
- If you receive a telephone request from a school, ask them to submit their request in writing and offer to forward their request to the student.

Potential employers

- Potential employers do not have an automatic right to information about the College's students.
- However, if a potential employer – or an agency conducting personnel checks for a potential employer – requests verification of a degree award, the College will provide this information as it is judged to be in the student's interest.
- The request must be in writing (fax or letter) on headed paper, and must include the student's name and information to be verified, such as the type and subject of the award.
- To ensure the information being verified is for the right person, it may be necessary to request the date of birth or year of the award.
- If staff receive a request by telephone or e-mail, they should ask the person making the request to submit it by fax or letter.
- If there is any question as to the genuineness of the request, staff should contact the student and obtain their permission to verify the award.
- Information other than verification of a degree award will not be provided without the student's consent.
- Requests for verification of an award will normally be handled by the Awarding Team (awarding@gsmlondon.ac.uk).

Council tax offices

- Confirmation of a person's status as a student will normally be made to council tax offices by the Student Centre.
- However, if the person requesting the information is a fraud investigator or works in a fraud investigation office, the request should be forwarded to the Data Protection Officer.

Police and other law enforcement bodies

- The police and other law-enforcement bodies do not have a right of access to information except where a particular Act obliges the College to provide information (e.g., Taxes Management Act) or a court order has been served.
- However, Section 29 of the Data Protection Act 1998 does allow for disclosure in certain situations where it is believed that not releasing the information would be likely to prejudice:
 - prevention and detection of crime;
 - apprehension or prosecution of offenders;
 - assessment or collection of taxes.
- If the police request information about a student, refer them to the Data Protection Officer. The Data Protection Officer will ask them to submit a data protection form. The form should state:
 - the identification of the student about whom they are requesting information;
 - the information they require;

- why the information is required (one of the purposes in Section 29 – see bullet points above);
- how the investigation would be prejudiced if the College does not supply the information;
- what the investigation is about (e.g., a named criminal investigation); and
- the signature of the investigating officer.
- Authorisation to release student information must be given by the Secretary to Board of Directors or his/her designated agents (Data Protection Officer or Records Manager) or the Chief Operating Officer or his/her designated agent(s) unless in exceptional circumstances (e.g., someone has committed a serious crime or it is believed a serious crime is about to be committed; or that the person may be a danger to him/herself or others), in which case information may be released directly.

Bailiffs

- Bailiffs do not have an automatic right to information about the College's students. Information must only be given if a court order is produced.
- If the bailiff produces a court order, information can be provided. However, the bailiff should be directed to the Data Protection Officer or the Secretary to the Board of Directors. The member of staff who deals with the request will ensure that copies of the information released, together with a photocopy of the court order and bailiff's identification, are kept.

Solicitors and other legal representatives

- If a solicitor or other legal representative requests access to a student's file, the request should be forwarded to the Information Access Officer.
- Such requests are normally accompanied by a signed release by the student, and are handled as subject access requests.

UK visas and immigration

- While UK Visas and Immigration (UKVI) (part of the Home Office) may have a right to information about the College's students, it is not an automatic right.
- They may request information to determine:
 - if a person is enrolled as a student at the College;
 - if a student is actually attending classes;
 - if a student has violated his/her visa conditions.
- In addition, they may ask for information to determine if a student is involved in terrorism by, for example, belonging to a prohibited organisation.
- If UKVI requests information by telephone, you should neither confirm nor deny if the person about whom they are asking is a student. You should ask the caller to make the request in writing, to the Data Protection Officer.

Media

- Enquiries from the media must be treated with care. Simply confirming that an individual is or has been a student at GSM London can be an offence under the Data Protection Act 1998.
- All media enquiries should be referred to the College's Press Office who will only release information regarding current and past students if the:
 - individual student has agreed that the information can be released;
 - information is already in the public domain;

- information must be released under the Freedom of Information Act 2000. In this case, information should only be released after consultation and agreement with the Data Protection Officer or Secretary to the Board of Directors.

Emergency disclosures

- The Data Protection Act 1998 allows for emergency release of information to protect the individual's 'vital interests', e.g.:
 - disclosure of a known medical condition if a student were unconscious;
 - serious concerns that a student may harm themselves or others (i.e., where there is serious risk that the College will fail in its duty of care towards the student or other students);
 - the student has been in contact with someone who has meningitis or other notifiable disease.
- The decision to release information should be taken by the Head of Department/College Dean, the Secretary to the Board of Directors or the Chief Operating Officer (or their designated agents).

Services bound by a professional code of ethics

Counselling and medical services

- Counselling and Medical Services staff will not pass on personal information about a student (including a student's attendance at counselling, disability or surgery appointments) to anyone outside the service subject to the following exemptions:
 - If Counselling and Medical Services staff have the express consent of the student to disclose the information.
 - If Counselling and Medical Services staff would be liable to civil or criminal court procedure if the information was not disclosed.
 - If Counselling and Medical Services staff believe the student, or other students or staff within the College, may be in serious danger.

Disability and Dyslexia Service

- Disability and Dyslexia Service staff will not pass on personal information about a student's disability/special need to anyone outside the service (including academic staff) without the student's express permission.
- If the student does not give their consent, the College will respect their decision but its implications regarding the level of support the College can provide will be made clear.

Placement and Careers Centre

- The Placement and Careers Centre staff operates according to the AGCAS Code of Practice on Guidance. It will not pass on personal information about a student without the student's permission.

International students

- All staff who provide guidance to international students will discharge their responsibilities in line with the Council for International Education/AISA code of ethics.