



Requests for Personal Data Procedures

© 2018 City of Glasgow College

Charity Number: SC0 36198

Table of Contents

1. Purpose	3
2. Scope	3
3. Responsibilities	5
4. Individual Rights under Data Protection Law	6
5. Requests for Personal Data by Third Parties	10
6. Security of Communications	14
7. Keeping an Audit Trail of Request	14
8. Further Help and Advice	15
9. Definitions	15
10. Monitoring and Measuring (optional)	15
11. Document Control and Review	16
12. Revision Log	17

1. Purpose

These procedures set out how to respond to requests for personal information which the College holds from and about:

- Prospective students;
- Current and former students;
- Current and former staff members;
- Other persons whose personal data we hold e.g. this could include CCTV images of a member of the public and visitor to the College.

These procedures set out how to deal with requests for personal data from the subject of the data and how to deal with requests for personal data from 3rd parties such as prospective employers and the police.

The procedures explain what a subject access request is (in terms of data protection legislation) and also when a request for personal data is not a subject access request.

2. Scope

2.1 What does this procedure cover?

The scope of these procedures applies to all personal information that we hold about all current and former City of Glasgow College (including all legacy colleges) students and staff, regardless of where or in what capacity they studied or worked within the College.

2.2 These procedures support the Data Protection Policy and other policies and procedures relating to the management of student and staff records and CCTV.

2.3 What is NOT covered by these procedures?

These procedures do not apply to routine requests for personal data from the subject of that personal data which we receive in the course of day to day

college business. More and more personal data is available to the data subject on a self-service basis through our systems such as MyCITY or iTrent which reduces the volume of requests we receive.

These procedures do not apply to requests for personal data (generally in bulk) which are passed by way of agreement to 3rd parties such as SFC, SDS and partners with whom we have legal agreements and clear legal grounds for information sharing. More information on the legal basis for information sharing is contained in the Data Privacy Notices for Staff and Students which are available on our website and updated regularly to ensure validity.

2.4 Student request for transcripts and certifications

These are requests which are limited and specific in scope to provide evidence of academic attainment or enrolment.

Current or former students may request an official transcript confirming their award and grades. This may include percentage marks. Students may also need an official certificate to confirm their period of enrolment at the College and any award or award date.

Both types of request should be managed by the Student Records team in accordance with the relevant College procedures and should not be treated as subject access requests unless they are part of a wider request for all data held by the College made by a particular individual.

3. Responsibilities

3.1 Data Protection Officer and Director of Corporate Support

Responsible for handling all subject access requests and all other requests in relation to personal rights under the Data Protection Act.

Responsible for providing legal and data management advice in relation to the operation of these procedures.

Responsible for liaison with the Information Commissioner where necessary.

3.2 Data Manager (at Curriculum Head or Service Head level)

Responsible for identifying subject access requests, authorising all routine requests for personal data and requests from 3rd parties for personal data.

Responsible for ensuring all relevant personal data is identified and provided to the Data Protection Officer for responses to Subject Access Requests or other rights requests made in relation to the Data Protection Act.

Responsible for the processing of student references (jointly with Head of Student Data and Research).

3.3 Head of Student Data and Research

Responsible for the management of centrally held student records and for processing requests for transcripts and certifications, for identifying subject access requests, authorising all routine requests for personal data and requests from 3rd parties for personal data.

Responsible for ensuring all relevant personal data is identified and provided to the Data Protection Officer for responses to Subject Access Requests or other rights requests made in relation to the Data Protection Act.

Responsible for the processing of student references (jointly with Faculties).

3.4 Director of HR

Responsible for the management of centrally held staff records and for identifying subject access requests, authorising all routine requests for personal data and requests from 3rd parties for personal data.

Responsible for ensuring all relevant personal data is identified and provided to the Data Protection Officer for responses to Subject Access Requests or other rights requests made in relation to the Data Protection Act.

Responsible for the processing of requests for staff references.

3.5 Vice Principal Infrastructure

Responsible for ensuring that all technical support is provided to the Data Protection Officer in order that the College can respond to rights requests made in relation to the Data Protection Act.

4. Individual rights under data protection law

Everyone has the right to know what personal information organisations hold about them, why and how their information is held and used, with whom their information is shared and for what purpose and for how long their personal information is retained.

People also have the following rights:

- To have their personal information amended where it is inaccurate
- To object to or to restrict processing of information that would cause them damage and distress
- To data portability and
- To seek erasure or rectification of their personal information.

Often requests such as these may follow a request for access to personal data. These requests can be complex and must be passed to the College's Data Protection Officer immediately for advice as to how the request should be handled. The Data Protection Officer may require may require ICT support and will alert the Vice Principal for Infrastructure if this is the case e.g. if there is a requirement for erasure that is deemed to be valid.

However, the most common request will be for access to personal information – this is called a Data Subject Access Request (SAR).

4.1 Handling data subject access requests

A formal request for a copy of one's own personal data is called a **Data Subject Access Request (SAR)**. A request does not have to specify that it is a data subject access request, or cite the Data Protection Act, for the request to be valid. The management of all such requests must be governed by a common set of rules which is the purpose of these procedures.

4.2 All requests must be made in writing

All requests should be made in writing and you should ask anyone who makes a verbal request to put their request in written form. However, if someone asks for assistance in completing a request, then we can provide help and the member of staff can complete the request and ask the applicant to confirm that the details are correct and to sign the request.

4.3 Proof of identification

If the person making the request for their own information (the Data Subject) is not known to the person receiving it, the Data Subject must provide proof of their identity in the form of their student ID card (smartcard), a birth certificate, passport or driving licence.

4.4 Requests made on behalf of the Data Subject by a third party

If someone makes a request on behalf of another person e.g. a parent on behalf of their child or lawyer on behalf of a client, the person making the request must provide evidence of their authority to make the request on behalf of the Data Subject, for instance confirmation of power of attorney, or the written consent of the Data Subject. If the member of staff receiving the request is in any doubt then it would be necessary to contact the Data Subject to get confirmation of their consent to the request to disclose their personal data. It may be more appropriate to send the personal data to the Data Subject rather than the person making the request on their behalf.

4.5 Fees for handling request

The College does not charge a fee for processing subject access requests.

4.6 Statutory timescales for complying with requests

The statutory deadline for responding to subject access requests is one calendar month from receipt of the request or from confirmation of the identity of the person making the request. If the request is very vaguely worded, it is legitimate to stop the clock at the point that the original request is received in order to seek clarification of the information requested.

4.7 Managing straightforward requests

If a request for personal data is straightforward and not contentious, it can be managed locally by the relevant Faculty or Support area, but only with the agreement of and advice from the Data Protection Officer.

For example:

A request received from a current/former student can be handled by Student Records or the relevant Faculty.

A request received from a current/former member of staff can be handled by Human Resources.

All requests require to be centrally logged by the Data Protection Officer's office for reporting and external monitoring purposes so the Data Protection Officer must be notified of all requests.

4.8 Managing more complex requests

It is essential that the Data Protection Officer manages any request which has one or more of the following characteristics:

- Complex or voluminous requests requiring retrieval and appraisal of information from various sources e.g. "all correspondence, emails, reports relating to my studies....."
- Requests made in the context of an appeal or dispute.
- Requests including information relating to other people (who will have their own rights as Data Subjects) within or out-with the College.
- Requests which combine a subject access (information about me) request with a FOISA request (information about the College e.g. How the College decided.....).

Under these circumstances, the Data Protection Officer will discuss the request with the Faculty or Support area that has received the request and agree how the request should be managed. It is essential that the operational area whose data is the subject of the request works and co-operates with the Data Protection Officer and ensures that the relevant information is identified to fulfil the request within the relevant timeframe. It is an offence to delete personal data once a SAR has been received from that individual.

The Data Protection Officer will review the information requested and advise what information should be disclosed or withheld in compliance with the relevant provisions of the Data Protection Act and any other relevant legislation e.g. Freedom of Information legislation.

5. Requests for personal data by third parties

These are not **subject access requests**. However, it is important to take care when disclosing personal data to third parties and these procedures set out the most common scenarios where requests are made in written form.

All requests for personal data by third parties should be authorised by a member of staff who is a Curriculum Head or Head of Service or above.

The member of staff releasing personal data will need to consider whether:

- The disclosure is necessary for the purpose claimed e.g. the prevention or detection of crime or the apprehension or prosecution of offenders; and
- Not disclosing the personal data would be likely to prejudice the purpose cited.

The responsible officer must be satisfied that the request is reasonable and proportionate and disclose only the minimum personal data necessary for the purpose, seeking advice from the Data Protection Officer as appropriate.

Where we have a contract with a partner or an existing legal relationship with them then the arrangements governing data sharing and personal data will be governed by that contract or data sharing agreement. The following procedures cover common scenarios where we do not have a contractual relationship with the 3rd party concerned e.g. the police or prospective employers of students and staff.

Remember that under most circumstances we must obtain the written consent of individuals before disclosing their personal data to third parties.

/5.1 ...

5.1 Third party requests to make contact with individuals

In this context the personal data of current or former students includes the fact that they are or were a City of Glasgow College student. If someone contacts the College asking to make contact with a current or former student expressing concern about their welfare we must not confirm that the person is nor was a student. We can offer to take the contact details of the enquirer and to forward these on to the individual concerned if our records confirm that they are or were at City of Glasgow College, in order that the individual can chose whether to respond.

5.2 Disclosure of information about students to sponsors or employers

In some cases a student may have signed an agreement at enrolment consenting to the disclosure of limited personal data necessary to confirm their status, attendance, progress and awards to a sponsor or potential employer. If evidence of consent is on record, in such a case it is legitimate to disclose the information requested as long as it is possible to verify that the person making the request:

- Is who they claim to be;
- Has the authority to make the request and;
- Has the consent of the applicant.

If in any doubt, seek the consent of the student.

5.3 Disclosure of information about staff: references

All requests for references must be handled by Human Resources. When receiving request for references about a current or former member of staff it is legitimate for us to disclose the limited personal data necessary to verify the details of their employment and role at the College to a potential employer, as long as it is possible to verify that the person making the request:

- Is who they claim to be;
- Has the authority to make the request; and
- Has the consent of the applicant.

If in any doubt, seek the consent of the Data Subject.

Staff need to be aware that Data Subjects have the right to ask the organisation that receives the reference for a copy of it. Both organisations and Data Subjects have the right to take legal action against the authors of references where they consider that the reference has misrepresented the candidate's abilities.

5.4 Disclosure of information about students: references

All requests for references received by the Student Records team are handled in accordance with their procedures and a signed mandate is required to be completed by the student making the request. These responses will simply confirm attendance and courses studied.

All requests received by Faculties can either be passed to the Student Records team for processing, if only basic attendance and course completion information is required, or handled by the Faculty. It is acknowledged that the Faculty may be asked and may provide more than the core data provided by the Student Records team. The Faculty must verify that the person making the request:

- Is who they claim to be;
- Has the authority to make the request; and
- Has the consent of the applicant.

If in any doubt, you must seek the consent of the Data Subject.

/Staff ...

Staff should be aware that Data Subjects have the right to ask the organisation that receives the reference for a copy of the reference. Both organisations and Data Subjects have the right to take legal action against the authors of references where they consider that the reference has misrepresented the candidate's abilities.

5.5 When someone claims legal authority to request personal data

In some cases, requests for personal data may be received from people claiming legal authority to ask for the information concerned. In these cases recipients of requests should seek advice from the Data Protection Officer.

Unless the person making the request has a warrant or court order requiring the College to disclose personal information about current or former students, the College is not obliged to comply with such requests. Therefore all staff who receive request for personal data from the Police or other government bodies must follow these procedures to ensure that disclosures of personal data are lawful, authorised, and accountable.

5.6 Requests from the Police

All requests for disclosure must be in writing, by email or letter. Organisations such as Police Scotland have a standard personal data request form. These requests must be:

- Signed by an officer with the authority to make the request; this may be an electronic signature or a scanned image of a signed form, if the request is made by email. The name and contact details of the requester and authoriser and the date of each signature must be clear on the form.
- Set out the legal authority for making the request. This is normally a specific section of the Data Protection Act. The request must explain how this right applies and why they need the information.

Even if the applicant is known to the person handling the request it is necessary to verify the applicant's identity and their authority to make the request.

6. Security of communications

All personal data disclosed in response to a request must be communicated by a method appropriate to the security and sensitivity of the information.

Before supplying information it is essential to check how the applicant wishes to receive the information and ensure that you have the correct postal or email address.

Information containing sensitive personal data sent by email or using a USB memory drive and/or other portable media devices must be encrypted.

If sending a hardcopy, then the packaging should be marked as '**Strictly Private and Confidential**' and sent via recorded delivery.

7. Keeping an audit trail of request

All subject access requests and requests from third parties must be recorded on the appropriate student or staff records system so that the College has an audit trail of actions taken in response to a request and can justify each decision. The record must include details of:

- the request;
- contact details of the applicant;
- evidence sought and obtained to verify their identity;
- the reasons for the decision and a copy of any information disclosed.

Keeping an audit trail ensures that staff can evidence and justify their decision to release personal data.

Records of Subject Access requests managed by the Data Protection Officer are held in the central data protection and FOISA management records.

The recommended retention period for the request records is completion plus 6 years in line with that for records that need to be retained for a limited time to defend the College's legal interest.

8. Further Help and Advice

For further advice and assistance contact

Data Protection Officer: Julia Henderson, Corporate Support Director

Julia.henderson@cityofglasgowcollege.ac.uk 0141 357 5535

9. Definitions

Data Protection Officer: the member of staff with oversight of organisational and technical measures and controls to comply with the Data Protection Act.

Personal Data: data which relates to a living person who can be identified from the data and other information that the Data Controller holds or is likely to receive.

Subject Access Request: A formal written request for a copy of one's own personal data.

Data subject: the owner of the personal data under consideration.

10. Monitoring and Measuring (optional)

Item	Target (e.g. deadline)
Time taken to process subject access requests	One calendar month

11. Document Control and Review

Approval Status	Approved
Approved by	SMT
Date Approved	2 May 2018
EQIA Status	EQIA Conducted? Yes
Proposed Review Date	2 May 2019
Lead Department	Corporate Support
Lead Officer(s)	Director of Corporate Support
Board Committee	Not relevant

12. Revision Log

Version Date	Section	Description