Audit & Assurance Committee

Date of Meeting	**Tuesday 11 June 2024**
Paper No.	**AAC4-C**
Agenda Item	**4.3**
Subject of Paper	**Data Protection Policy and EqIA**
FOISA Status	**Disclosable**
Primary Contact	**Dr Sheila Lodge** **Depute Principal & Chief Operating Officer**
Date of production	**21 May 2024**
Action	**Discussion and Decision**

1. Recommendations

1.1 The Committee is asked to approve the updated Data Protection Policy and its accompanying Equality Impact Assessment (EqIA).

2. Purpose

2.1 The purpose of this paper is to secure the Committee's approval for the revised Data Protection Policy (and its accompanying EqIA).

3. Consultation

3.1 The Policy and EqIA have been revised by the Data Protection Officer, who has consulted the Depute Principal & Chief Operating Officer. They were approved by SMT at its meeting on 13 March 202, and by Academic Board at its meeting on 20 May 2024.

4. Key Insights

4.1 The College's Data Protection Policy was due for review in November 2023. This review has now been completed by the Data Protection Officer.

4.2 There are no substantive changes to the Policy, but the opportunity has been taken to implement minor amendments that make the document clearer and more user-friendly. Key roles and responsibilities have also been updated in keeping with the organisational changes made last year.

4.3 The Policy is accompanied by its revised Equalities Impact Assessment.

5. Impact and Implications

5.1 The College must comply with the UK General Data Protection Regulation (GDPR), UK Data Protection Act, 2018 (DPA) and all and any other relevant legislation protecting privacy rights ("data protection law"), including that of other jurisdictions in which the College operates.

5.2 The Data Protection Policy captures how the College will fulfil its legal responsibilities, and is a key document in evidencing City's compliance.

Appendices

Appendix1: Data Protection Policy, V4.1

Appendix 2: Equalities Impact Assessment

Data Protection Policy

City of Glasgow College
Charity Number: SCO 36198

Table of Contents

1. Introduction

City of Glasgow College ('the College') is a learning institution with an international reach. The College values its individual learners and we seek to demonstrate integrity, honesty and transparency in the delivery of inspirational and personalised learning and teaching. The personal data of our students and staff is one of our core assets. The College must comply with the UK General Data Protection Regulation (GDPR), UK Data Protection Act, 2018 (DPA) and all and any other relevant legislation protecting privacy rights ("data protection law"), including that of other jurisdictions in which the College operates. This policy applies to all processing of personal data by and for the College, regardless of where the processing takes place.

The College is a data controller, which means it makes decisions about the reasons why it collects personal data from individuals, how it uses the data and who it shares it with. The College is legally responsible for all decisions it makes about its use of personal data and must ensure that all of its processing of personal data is conducted in accordance with the requirements of data protection law.

1.1 Data Protection Officer

The College has appointed a Data Protection Officer to advise the organisation on its obligations to comply with data protection law. The Data Protection Officer can be contacted to provide support with any data protection questions at dpo@cityofglasgowcollege.ac.uk.

2. Purpose and Aims

2.1. This policy provides practical guidance to all staff on their responsibility to process personal data in accordance with data protection law. It explains how the College uses personal data and why, and the procedures and controls the College has in place to protect personal data.

2.2. The policy explains how the College demonstrates its compliance with the principles of data protection law.

In summary, these state that personal data shall be:

- processed lawfully, fairly and in a way that is transparent and explained to the individuals ("lawfulness, fairness and transparency");
- collected or created for specified, explicit and lawful purposes and not be further processed in a manner that is incompatible with those purposes. ("purpose limitation");
- adequate, relevant and limited to what is necessary for those purposes ("data minimisation");
- accurate and kept up to date ("accuracy");
- retained in a form that can identify individuals for no longer than is necessary for that purpose ("storage limitation"); and
- kept safe from unauthorised access, processing, accidental or deliberate loss or destruction ("integrity and confidentiality")
- the College shall maintain records, policies and procedures which demonstrate its accountability with data protection law ("accountability").

3. Scope

3.1 This policy sets out and explains the framework of governance and accountability for data protection compliance across the College.

3.2 It applies to all personal data, which is information that could be used to identify and individual. Individuals include, but are not limited to:

- prospective applicants,
- applicants to programmes and posts,
- current and former students,
- alumni,
- current and former employees,
- family members where emergency or next of kin contacts are held,
- workers employed through temping agencies,
- members of the Board and members of the Committees of the Board,
- visiting academics and volunteers,
- potential and actual donors,
- customers,
- conference delegates,
- people making requests for information or enquiries,
- complainers,
- professional contacts and
- representatives of funders, partners and contractors.

3.3 Personal data may include basic identifiers such as name, address, email address and images, such as this captured on CCTV or ID cards. It includes special category personal data, which is more sensitive and includes health information and data about ethnicity, religious beliefs, trade union membership and sexual orientation. It applies to processing of electronic records and physical paper records.

3.4 Applicability of this policy

This policy applies to the processing of personal data at all College locations, including locations outside the UK and personal data processed remotely, for example, by staff working from home.

It applies to all staff that process personal data at work and any contractors working on behalf of the College.

4. Policy Statement

The College will comply with Data Protection Principles and all other requirements of data protection law, ensuring that personal data with which the College is entrusted is processed fairly and securely.

4.1 We will process personal data fairly and lawfully

This means that we will:

- only collect and use personal data in accordance with the lawful principles set down under the GDPR;
- treat people fairly by using their personal data for purposes and in a way that they would reasonably expect;
- ensure that if we collect someone's personal data for one purpose e.g. to provide advice on study skills, we will not reuse their data for another incompatible purpose e.g. to promote goods and services for an external supplier; and
- rely on consent as a condition for processing personal data only where:
  - we first obtain the data subject's specific, informed and freely given consent;
  - the data subject gives consent, by a statement or a clear affirmative action that we document; and

- the data subject must be able to withdraw their consent at any time with the same ease with which they gave consent and without detriment to their interests.

4.2 We will inform Data Subjects about what we are doing with their personal data

This means that at the point that we collect their personal data, we will explain to Data Subjects in a clear, concise and accessible way:

- what personal data we collect;
- for what purposes we collect and use their data;
- what lawful conditions we rely on to process data for each purpose and how this affects their rights;
- whether we intend to process the data for other purposes and their rights to object;
- the sources from which we obtain their data, where we have received the data from third parties;
- whether we use automated decision making, including profiling, and if so the impact on data subjects and their rights to object;
- whether they need to provide data to meet a statutory or contractual requirement;
- our obligations to protect their personal data;
- to whom we may disclose their data and why;
- where relevant, what personal data we publish and why;
- how data subjects can update the personal data that we hold;
- how long we intend to retain their data;
- how to exercise their rights under data protection law; and
- the identity and contact details of the Data Protection Officer.

We will publish this information on our website and where appropriate in printed formats. We will review the content of these Privacy Notices regularly and inform our data subjects of any significant changes that may affect them.

We will provide simple and secure ways for our students, staff and other data subjects to update the information that we hold about them e.g. home addresses. Where we process personal data to keep people informed about College activities and events we will provide in each communication a simple way of opting out of further marketing communications.

Through these actions we demonstrate both accountability for our use of personal data and that we manage people's data in accordance with their rights and expectations.

4.3 We will uphold individual's rights as data subjects

This means that we will uphold their rights to:

- obtain a copy of the information comprising their personal data, free of charge within one month of their request;
- have inaccurate personal data rectified and incomplete personal data completed;
- have their personal data erased when it is no longer needed, if the data have been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data;
- restrict the processing of their personal data until a dispute about the data's accuracy or use has been resolved, or when the College no longer needs to keep personal data but the data subject needs the data for a legal claim;
- data portability (if applicable): where a data subject has provided personal data to the College by consent or contract for automated processing and asks for a machine-readable copy or to have the data sent to another data controller;
- object to and prevent further processing of their data for the legitimate interests or public interest unless the College can demonstrate compelling lawful grounds for continuing;
- prevent processing of their data for direct marketing;

- object to decisions that affect them being taken solely by automated means (if applicable); and
- complain to the Information Commissioner's Office if unhappy about the way the College processes their personal data.

A data subject may exercise any of the above rights by making a request to any member of College staff verbally, in writing or by other means such as social media. We normally have 1 month to respond to a request and we typically do not charge a fee. All requests must be reported to dpo@cityofglasgowcollege.ac.uk without delay.

4.4 We will apply "data protection by design and default" principles to all our personal data processing

This means that we will:

- consider privacy at the heart of what we do and 'bake' data protection into our operations;
- use proportionate privacy and information risk assessment, and where appropriate data protection impact assessment, to identify and mitigate privacy risks at each stage of every project or initiative involving the processing personal data and in managing upgrades or enhancements to systems and processes used to process personal data;
- seek advice from dpo@cityofglasgowcollege.ac.uk before engaging in a new project, research activity or a new partnership which will involve the processing of personal data;
- adopt data minimisation: we will collect, disclose and retain the minimum personal data for the minimum time necessary for the purpose; and
- anonymise personal data wherever necessary and appropriate, e.g. when using it for statistical purposes, so that individuals can no longer be identified.

4.5 We will protect personal data

This means that we will use appropriate technical and organisational measures to:

- control access to personal data so that staff, contractors and other people working on College business can only see such personal data as is necessary for them to fulfil their duties;
- require all College staff, contractors, students and others who have access to personal data in the course of their work to complete basic data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles;
- set and monitor compliance with security standards for the management of personal data as part of the College's wider framework of information security policies and procedures;
- reduce risks of disclosure by pseudonymsing personal data where possible;
- provide appropriate tools for staff, contractors, students and others to use and communicate personal data securely when working away from the College, for instance through provision of a secure Virtual Private Network, encryption and cloud solutions;
- take all reasonable steps to obtain assurance that all suppliers, contractors, agents and other external parties who process personal data for the College will comply with auditable security controls to protect our data and enter into our standard contracts in accordance with our procurement policies and procedures;
- maintain data sharing agreements with educational partners and other external bodies with whom we may need to share personal data to deliver academic programmes, shared services or joint projects to ensure proper governance, accountability and control over the use of such data;
- where transferring personal data to another country outside the UK put in place appropriate agreements and auditable security controls to maintain privacy rights;
- ensure that our students are aware of how data protection law applies to their use of personal data in the course of their studies and how they can

take appropriate steps to protect their own personal data and respect the privacy of others;

- manage all subject access and third party requests for personal information about staff, students and other data subjects in accordance with our procedures for responding to requests for personal data; and
- make appropriate and timely arrangements to ensure the confidential destruction of personal data in all media and formats when it is no longer required for College business.

4.6 We will retain personal data only for as long as required

This means that we will:

- apply the College's records retention schedules to keep records and information containing personal data only so long as required for the purposes for which they were collected;
- apply exemptions to public rights of access to information as appropriate in accordance with the data subjects' rights to privacy; and
- redact personal data where information is only required for statistical purposes e.g. by pseudonymisation.

4.7 We will manage any breaches of data security promptly and appropriately

This means that we will take all necessary steps to reduce the impact of incidents involving personal data by following the College data breach procedures. All suspected breaches much be reported immediately to dpo@cityofglasgowcollege.ac.uk and ITsupport@cityofglasgowcollege.ac.uk without delay in order that IT and the DPO may work together to assess the risk.

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will liaise with the Information Commissioner's Office and report the breach, in line with regulatory requirements, within **72 hours** of discovery. The Data Protection Officer will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

6. Responsibilities

6.1 All staff who access and use College personal data are responsible for:

6.2 The Principal, as the Chief Executive Officer of the College, has ultimate accountability for the College's compliance with data protection law and for ensuring that the Data Protection Officer is given sufficient autonomy and resources to carry out their tasks effectively.

6.3 The Vice Principal of People and Corporate Support has senior management accountability for information governance and legal advice.

6.4 The Data Protection Officer is responsible for:

- informing and advising senior managers and all members of the College community of their obligations under data protection law;
- promoting a culture of data protection, e.g. through training and awareness activities;
- reviewing and recommending policies, procedures, standards, and controls to maintain and demonstrate compliance with data protection law and embed privacy by design and default across the College;
- advising on data protection impact assessment and monitoring its performance;
- monitoring and reporting on compliance to the Executive and the Audit and Risk Committee, the Board and other committees as appropriate;
- convening meetings of the Data Management group;
- ensuring that Records of Processing and 3rd party sharing activities are maintained;
- providing a point of contact for data subjects with regard to all issues related to their rights under data protection law;
- investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence;
- acting as the contact point for and cooperating with the Information Commissioner’s Office on issues relating to processing;

The Data Protection Officer will:

- monitor new and on-going data protection risks and update the relevant risk register; and
- make regular reports to the College Executive and other Committees and Boards on data protection compliance.

The Data Protection Officer at the College may be contacted at dpo@cityofglasgowcollege.ac.uk. Other arrangements may be made for oversight of these duties.

6.5 All Faculty Deans and Support Services Directors are responsible for implementing this policy within their business areas, and for adherence by their staff.

This includes

- assigning generic and specific responsibilities for data protection management;
- managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such personal data is necessary for them to fulfil their duties;
- ensuring that all staff in their areas of responsibility undertake a relevant and appropriate training and are aware of their responsibilities for data protection;
- ensuring that staff responsible for any locally managed IT services liaise with College's ICT staff to put in place equivalent IT security controls;
- assisting the Data Protection Officer in maintaining accurate and up to date records of data processing activities;
- ensuring that they and their staff cooperate and support the Data Protection Officer in relation to subject access requests and other requests relating to personal data where the data is owned and managed by their business area; and
- recording data protection and information security risks on their local risk registers and escalating these as necessary.

6.6 The Chief Finance Officer is responsible for:

- ensuring that centrally managed IT systems and services embed privacy by design and default and for promoting good practice in IT security among staff; and
- ensuring, in conjunction with the Data Protection Officer, that IT security risks related to data protection are captured on the College risk register.

6.8 The Head of Estates is responsible for ensuring that controls to manage the physical security of the College, including CCTV, take account of relevant data protection laws and risks.

6.9 The Director of People and Culture is responsible for maintaining relevant human resources policies and procedures, to support compliance with data protection law.

6.10 The Head of Student Data is responsible for maintaining relevant student administration policies and procedures and for oversight of the management of student records and associated personal data across the College in compliance with data protection law.

6.11 The College Secretary is responsible for ensuring that data protection and wider Information Security controls are integrated within risk management and audit programmes.

6.12 The Associate Director of Procurement is responsible for ensuring that supply chain due diligence and procurement processes embed information risk and data protection impact assessment and privacy by design.

6.13 As part of the College's internal audit programme, the Audit Committee will instruct the College's Internal Auditors to audit the management of privacy and data protection risks and compliance with relevant controls, as required.

7. References

7.1 Other College Policies and Procedures

Policy / Procedure	Title
Procedure	Records Management Schedules.
Procedure	Data Breach Procedure.
Procedure	Request for Personal Data Procedure.
Legal Notice	Privacy Notice for Students.
Legal Notice	Privacy Notice for Staff.
Legal Notice	Data Protection Quick Guide

7.2 External References

Source	Title
ICO	Guide to data protection.

8. Document Control and Review

Approval Status	Approved		
Approved by	Audit Committee		
Date Approved	20/11/2019		
EQIA Status	EQIA Conducted?	Yes:	No:
Proposed Review	20/11/2023		
Board Committee	Audit Committee		

9. Revision Log

Version Date	Section of Document	Description of Revision
Version 2 20/112019		Second Version of City of Glasgow College ' Data Protection Policy.
FEB 2021		Third version of Data Protection Policy. Updates made in respect of Brexit.
Aug 2022 3.1 version		Name update and review date renewal
February 2024 Version 4		Revision of policy to make it more user friendly and clear for staff and updates to internal roles and responsibilities.

Equality Impact Assessment (EQIA)

The General Equality Duty and protected characteristics are detailed at the end of this form.
Refer to the EQIA Guidance Document for more Information on how to complete this form.

Title of Policy, Procedure, or Relevant Practice:	Data Protection Policy	
Lead Officer:	Sheila Lodge	
Type of Policy, Procedure, or Relevant Practice:	Data Protection New:	Existing
Date of Assessment:	19 February 2024	

Step1: Outcomes and Potential Impacts
1A. What are the intended consequences (outcomes) of the policy, procedure or relevant practice? **The Data Protection Policy/Procedures must be in place to enable the College to demonstrate accountability with its Data Protection obligations. The policy applies to the processing of any personal data by the College and it is the overarching policy document for data protection. It provide all colleagues that process personal data with guidance and information about their obligations when processing personal data while discharging their duties as employees of the College.**
1B. Could this policy, procedure or relevant practice potentially result in differential impact on groups with protected characteristics? No

Step 2: Consideration of Evidence and Information
2A. What information do you plan to use as the basis of this EQIA? (What information is available and if information is lacking, how will you address this shortfall?) **N/A**
2B. Please indicate potential positive, neutral and negative impacts in relation to each protected characteristic. (What does the information indicate about potential positive, neutral and negative impacts on people who share protected characteristics? Are the needs of people with different characteristics met? Does the policy, procedure, or relevant practice affect some groups differently?)

Protected Characteristic	Detail the Potential Positive, Neutral, or Negative Impacts with Reference to Evidence, or Information
Age	N/A

2B. cont'd

Protected Characteristic	Detail the Potential Positive, Neutral, or Negative Impacts with Reference to Evidence, or Information
Disability	N/A

Gender Reassignment	N/A
2B. cont'd	
Protected Characteristic	**Detail the Potential Positive, Neutral, or Negative Impacts with Reference to Evidence, or Information**
Marriage & Civil P'ship *	N/A

Pregnancy & Maternity	N/A
2B. cont'd	
Protected Characteristic	**Detail the Potential Positive, Neutral, or Negative Impacts with Reference to Evidence, or Information**
Race	N/A

Religion or Belief	N/A
2B. cont'd	
Protected Characteristic	**Detail the Potential Positive, Neutral, or Negative Impacts with Reference to Evidence, or Information**
Sex	N/A

Sexual Orientation	N/A

Step 3: Consider Alternatives and Mitigation
3A. Are you able to reduce any potential negative impacts identified above? Yes: ☐ No: ☐ N/A: ☐ **If N/A, go to Step 4**
3B. If "Yes", what arrangements could be implemented to reduce any potential negative impacts identified above? N/A

3C. If "No", it may be appropriate if the policy, procedure, or relevant practice affects groups differently where this is a proportionate means of achieving a legitimate aim. If this is the case, please provide explanatory details to objectively justify this decision. **(Note: you may be required to obtain legal advice to verify your decision. If you suspect this may be the case, please contact Diversity & Equalities for direction.)**

Step 4: Compliance with General Equality Duty
4A. Does the policy, procedure or relevant practice comply with the three parts of the general duty: • **Eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by the Act.** • **Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.** • **Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.** Yes: ☐ No: ☐ **For 4B- 4D, please detail relevant groups who share a protected characteristic and refer to evidence/information**
4B. If "Yes", how?
4C. If "No", what are the negative impacts and the associated risks?
4D. If "No", What arrangements exist, or could be implemented to better comply with the general duty?

Step 5. The Involvement of Individuals, Groups and Organisations Representing Protected Characteristics
5A. Who has been involved in the undertaking of this assessment? (Please detail the staff/student/stakeholder groups) N/A
5B. How successful has this been, and what changes can be made to improve this process in the future? N/A
5C. If you have further involvement to carry out, please list who you are going to involve and how? N/A

Step 6: Making a decision and outcome
6A. What is your decision? (Please select an option from the drop down menu options using the arrow on the right) **A.** A positive impact is explicitly intended and very likely.

B. A negative impact is not foreseen, and on the contrary the policy has the clear potential to have a positive impact by reducing and removing barriers and inequalities that currently exist. **C.** A negative impact is not foreseen. On the contrary there is potential to reduce barriers and inequalities that currently exist. There is insufficient evidence, however, for this assessment to be made with as much confidence as is desirable. **D.** A negative impact is not foreseen, but positive impact is also unlikely. [X] **E.** A negative impact is probable or certain, since certain groups will be disadvantaged, either proportionately or absolutely, or both. Remedial action is therefore necessary. **F.** A negative impact is probable or certain for some groups but the policy as a whole can nevertheless be justified as a **proportionate means of achieving a legitimate aim.** **Note: you may be required to obtain legal advice to verify your decision. If you suspect this may be the case, please contact Diversity & Equalities for direction.**
6B. Are you able to introduce the policy, procedure, or relevant practice without making any changes? Yes: ☒ No: ☐
6C. If "Yes", clearly explain upon which basis this decision was made **This is an existing policy which has been in place since 2018. It is updated at least every 2-years.**
6D. If "No", what changes will you make before implementation?

Step 7: Taking action and monitoring
7A. What action will we take? 1. This policy and procedure should be shared with Department and Faculty Heads as a reminder of the obligation to follow the required process and guidance within their business areas. 2. Department and faculty reviews to monitor compliance with this policy and procedure will be undertaken between February 2024 and June 2024. 3. This policy is reviewed annually to ensure it is accurate and up to date.
7B. Who will take that action? COO and DPO
7C. When will that action be completed? 1. To be agreed with CCO 2. From February 2024
7D. Once implemented, how will the policy, procedure, or relevant practice be monitored? Annually with updates made on an annually or every 2-years as required.

Miscellaneous Additional Information (please insert any supporting information, or data here)

Sign-off, authorisation and publishing	
For College records, but not for publishing publicly • The information contained within this EQIA needs to be confirmed and approved as the completed EQIA will be published on the College web-site. • As such, EQIAs must be approved by a Director or above. • Ask a Director to review and sign off the EQIA (an electronic signature will suffice, as long as a paper copy follows). • Following completion, send an electronic copy to both the Diversity & Equalities Manager and Director of Planning and Administration.	
Name:	
Position:	
Signature:	
Date:	

CITY OF GLASGOW COLLEGE

Summary of the General Duty of the Equality Act 2010

Components A public authority must, in the exercise of its functions, ***have due regard*** to the need to:	**Due Regard** Having due regard specifically involves taking steps to:
a) Eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by the Act.	
b) Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.	a) Remove or minimise disadvantages suffered by persons who share a relevant protected characteristic that are connected to that characteristic ***** b) Take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it. c) Encourage persons who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such persons is disproportionately low.
c) Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.	a) Tackle prejudice. b) Promote understanding.

'Due regard' comprises two linked elements: proportionality and relevance. The weight that public authorities give to equality should be proportionate to how relevant a particular function is to equality. In short, the more relevant a function is to equality, then the greater the regard that should be paid.

The protected characteristics are:

- Age
- Disability
- Gender reassignment
- Marriage and Civil Partnership *****
- Pregnancy and Maternity
- Race
- Religion or Belief
- Sex
- Sexual Orientation

***** Although Marriage and Civil Partnership applies to section a) in employment only, this will be considered for **all** stakeholders