Board of Management

Date of Meeting	**Wednesday 6 June 2018**
Paper No.	**BoM6-O**
Agenda Item	**17.2.1**
Subject of Paper	**Data Protection Policy**
FOISA Status	**Disclosable**
Primary Contact	**Julia Henderson, Director of Corporate Support**
Date of production	**9 May 2018**
Action	**For Noting**

1. Recommendations

The Board is asked to note the new Data Protection policy as approved by the Audit Committee on 16 May 2018.

Board of Management

Audit Committee

Date of Meeting	**Wednesday 16 May 2018**
Paper No.	**AC4-B**
Agenda Item	**5**
Subject of Paper	**Data Protection Policy**
FOISA Status	**Disclosable**
Primary Contact	**Julia Henderson, Director of Corporate Support**
Date of production	**9 May 2018**
Action	**For Approval**

1. Recommendations

Committee is asked to approve the new Data Protection policy.

2. Purpose of report

The Report seeks Committee's approval of the new Data Protection policy, which has been completely refreshed to comply with the new data protection legislation. The General Data Protection Regulations (GDPR) come into force on 25 May 2018 and the UK Act is currently passing through the House of Lords.

At its meeting on 30 April, the Performance, Remuneration and Nominations Committee received a full update on progress made by the College to implement GDPR. The Audit Committee will have before them the Internal Audit Report on GDPR implementation for reference.

As agreed with the Chair of the Board, a full report will go to the next Board Meeting on 6 June 2018, to ensure that all members are aware of the College's responsibilities under the GDPR.

3. Strategic Context

In August 2017 the Senior Management team agreed their approach in relation to the new law:

To take the time to properly prepare for and comply with the new laws, both to avoid the risk of significant fines and reputational damage, but, and in many ways more importantly, to take advantage of the opportunity to improve our data handling, our information security systems and our compliance processes and to ensure that our contractual staff and student relationships are professional, robust and reliable.

The policy and its associated procedures support College compliance with its obligations as a Data Controller and, where applicable, a Data Processor, under data protection law.

4. Discussion

The new College Data Protection policy and procedures relating to personal data requests and data breach were discussed at the Senior Management Team on 3 May 2018. As is appropriate the SMT approved the new procedures.

The policy makes clear that, since processing personal data is central to what we all do on a daily basis, staff have a responsibility to look after personal data and comply with the law. The policy sets out the specific responsibilities of key staff members. The new procedures sit alongside the policy and our new privacy notices for staff and students.

A new dedicated page has been created on the College website for Data Protection and all relevant information, including the policy, will sit on this page.

5. Impact and implications

We should have an approved policy setting out our core compliance responsibilities in place for 25 May 2018.

Where we fail to comply there are clear reputational and financial risks for the College, both with external stakeholders and with our staff and students. The new law is multifaceted but key changes include:

- more significant organisational fines and investigatory powers for the ICO;
- requirement for organisations to more proactively inform individuals what they do with their personal data and how they look after it;
- requirement to report data breaches within 48 hours;
- new responsibilities for organisations managing personal data; and
- improved rights for individuals in relation to their personal data.

Data Protection Policy

City of Glasgow College
Charity Number: SCO 36198

Table of Contents

1. Introduction

City of Glasgow 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 our core asset. The College must comply with the European Union General Data Protection Regulation (GDPR), UK Data Protection Act, 2018 (DPA) and other relevant legislation protecting privacy rights. This policy applies to all processing of personal data by and for the College, regardless of where the processing takes place.

The College must also comply with relevant legislation in other jurisdictions where the College operates.

These data protection laws require the College to protect personal information and control how it is used in accordance with the legal rights of the data subjects - the individuals whose personal data is held.

2. Purpose and Aims

2.1. This policy and its associated procedures and guidance support College compliance with its obligations as a Data Controller and, where applicable, a Data Processor under data protection law.

2.2. The College is responsible for, and must be able to demonstrate, compliance with the following Data Protection Principles ("accountability").

2.3. In summary, these state that personal data shall be:

- processed lawfully, fairly and in a way that is transparent to the data subject ("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").

2.4. Under data protection law the College must also:

- proactively inform data subjects about its data processing activities and their rights under the law;
- meet its legal obligations as a data controller or processor, including: ensuring that data protection is 'designed in' to its processes by default; that we carry out data protection impact assessment; that we maintain records of processing activities; that we take measures to ensure the security of processing and the proper handling of data breaches; and that

we have identified an appropriately qualified and senior Data Protection Officer; and

- allow personal data to be transferred to other countries only if it maintains the same level of protection for the privacy rights of the data subjects concerned.

3. Scope

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

3.1. What information is included in the policy

This policy applies to all personal data created or received in the course of College business in all formats, of any age. Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone.

3.2. Who is affected by the policy

3.2.1 Data subjects

These include, but are not confined 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.

3.2.2 Users of personal data

The policy applies to anyone who obtains, records, can access, store or use personal data in the course of their work for the College. Users of personal data include employees and students, contractors, suppliers, agents, College partners and visitors.

3.3 Where the Policy applies

This policy applies to all locations from which College personal data is accessed including home use.

As the College operates internationally, through arrangements with partners in other jurisdictions, the policy applies to international activities.

4. Policy Statement

The College will apply the Data Protection Principles and the other requirements of data protection law to the management of all personal data throughout the information life cycle by adopting the following policy objectives.

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 a different purpose that the individual did not agree to or expect 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 can withdraw their consent at any time without detriment to their interests.

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

This means 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;
- the identity and contact details of the Data Protection Officer; and

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

- claim compensation for damages caused by a breach of data protection law.

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

This means that we will:

- 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 processing personal data and in managing upgrades or enhancements to systems and processes used to process 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 European Union 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 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;
- redact personal data, e.g. by pseudonymisation; and
- withhold access to specific categories of record, such as student records, for the lifetime of the student and their identifiable next of kin.

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 data breach procedures.

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.

5. 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 living individual whose personal data we hold.

Data Controller: any person who determines the purposes for which and the manner in which any personal data is to be processed. For the purposes of this policy the College is the data controller.

Data Processor: in relation to personal data, means any person (other than an employee of the data controller) who processes data on behalf of the data controller.

6. Responsibilities

6.1 All users of College information are responsible for:

- completing relevant training and awareness activities provided by the College to support compliance with the Data Protection policy and relevant procedures;
- taking all necessary steps to ensure that no breaches of information security result from their actions;
- reporting all suspected information security breaches or incidents promptly to ICTHelpdesk@cityofglasgowcollege.ac.uk so that appropriate action can be taken to minimise harm; and
- informing the College of any changes to the information that they have provided to the College in connection with their employment, for instance, changes of address or bank account details.

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 Director of Corporate Support has senior management accountability for information governance and legal advice and is the College's Data Protection Officer.

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 role may be filled by the Director of Corporate Support or other arrangements may be made for oversight of these duties.

6.5 All Faculty Directors and Support Services Directors are responsible for implementing the 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 Vice Principal Infrastructure 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.

6.7 The Data Management Group is responsible for:

- promoting a culture of data protection compliance across the College and within their area of responsibility;
- acting as a professional and practitioner support network for the data protection officer;
- recommending policy, procedural and systems improvements and changes to maintain and demonstrate compliance with data protection law and embed privacy by design and default across the College; and
- ensuring that Records of Processing and 3rd party sharing activities are maintained in their area of responsibility.

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 Human Resources is responsible for maintaining relevant human resources policies and procedures, to support compliance with data protection law.

6.10 The Head of Student Data and Research 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 Procurement Manager 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 Note for Staff.

7.2 External References

Source	Title
ICO	Guide to data protection.

8. Document Control and Review

Approval Status		
Approved by		
Date Approved		
EQIA Status	EQIA Conducted?	Yes: ☒ No: ☐
Proposed Review Date		
Lead Department		
Lead Officer(s)	Julia Henderson, Director of Corporate Support	
Board Committee	Audit Committee	
Copyright © 2012 City of Glasgow College	Permission granted to reproduce for personal use only. Commercial copying, hiring lending, posting online is strictly prohibited.	

9. Revision Log

Version Date	Section of Document	Description of Revision
Version 0 DD MMM YYYY		First Version of City of Glasgow College ' Data Protection Policy.