Data Protection Policy

I. Policy

The role of Glasgow Colleges' Regional Board (GCRB) is to secure the coherent provision of a high quality of fundable further and higher education in Glasgow's colleges. GCRB's functions include administration of funds; planning and performance monitoring of Colleges, including efficiency studies; improvement of economic and social well-being; transfer and property of staff; and appointment of Board Members.

To fulfil these functions, GCRB collects and processes data for:

1. Appointment and employment purposes in relation to its staff and Board Members;
2. Ensuring safety of visitors;
3. Administration of funds from the Scottish Government to its Colleges;
4. Reporting to the Scottish Government on the administration of funds, including forecasting and monitoring of College spend.
5. Handling complaints, Freedom of Information Requests, Data Subject Access Requests, Whistleblowing concerns and other procedures that it may be required to undertake as a public authority.

GCRB must comply with the European Union General Data Protection Regulation (GDPR), UK Data Protection Act, 2018 (DPA) and other relevant legislation protecting the privacy rights of individuals whose data it processes.

This policy applies to all processing of personal data by and for GCRB, regardless of where the processing takes place. GCRB takes its data protection responsibilities seriously and is committed to protecting the personal data it processes by ensuring that the information is kept secure, accurate and up-to-date in accordance with the legal rights of the data subjects (the individuals on which the personal data is held).

Please note that, aside from appointment, employment and visitor purposes, most of the data processed by GCRB in its day-to-day business is anonymised and does not contain personal data, for example in the administration of funds or for reporting purposes.

II. Scope

This policy has been developed to support the rights of the data subjects by setting out a framework of governance and accountability for data protection compliance and applies to:

1. all Board members, staff, contractors and partners working for or on behalf of GCRB;
2. all personal data created, collected, stored, adapted, transferred, erased, destroyed and otherwise processed through any GCRB activity. Personal data may be held or shared in paper and electronic formats including email or communicated verbally in conversation or by phone;
3. all locations from which GCRB personal data is accessed, including home use.

III. Definitions

Personal data: any information relating to a living person who can be identified (directly (e.g. by name) or indirectly (e.g. by circumstance)).

Data subject: the living individual to whom the personal data relates. This includes, but is not limited to prospective, current and former employees and Board members, visitors, family members where emergency and next of kin contacts are held, volunteers, event delegates.

Data controller: any person, public authority, agency or other body that determines the purposes and way in which any personal data is processed. For the purposes of this policy, GCRB is the data controller.

Processing: any operation or set of operations performed on personal data including collection, organising, storing, adapting, retrieving, transmitting, sharing, erasing or destroying.

Data Subject Request: Any request by a data subject to be informed, access, rectify, delete, restrict or object to processing of their data and also requests around data portability and those related to automatic decision making. The most common request is a 'subject access request', where the data subject asks for a copy of their personal data.

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

Special Category Personal Data: 'sensitive' information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data used to identify an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

IV. Responsibilities

1. All users of GCRB personal, special category 'sensitive' data and confidential information (staff, Board members and other users) are responsible for:
   a) completing relevant training and awareness activities provided by GCRB to support compliance with the Data Protection policy and relevant procedures;
   b) treating all personal data as confidential;
   c) taking all necessary steps to ensure that no breaches of information security result from their actions;
   d) reporting all suspected information security (data) breaches or incidents promptly to GCRB's Data Protection Officer so that appropriate action can be taken to minimise harm;
   e) informing GCRB of any changes to the information that they have provided in connection with their relationship with GCRB, for instance, changes of address or bank account details;
   f) assisting the Data Protection Officer in maintaining accurate and up to date records of data processing activities;
   g) cooperate and support the Data Protection Officer in relation to subject access and other requests relating to personal data where the data is managed by them; and
   h) recording data protection and information security risks on the Risk Register and escalating these as necessary.
2. The Executive Director of GCRB has ultimate accountability for compliance with data protection law, responsible for information governance and for ensuring that the Data Protection Officer is given sufficient autonomy and resources to carry out their tasks effectively.
3. The Data Protection Officer is responsible for:

- informing and advising all employees and members of GCRB of their obligations under data protection law;
- promoting a culture of data protection, 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 GCRB;
- advising on and monitoring data protection impact assessments;
- monitoring and reporting on compliance to the Board as appropriate;
- 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 incidents and 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;

V. Policy statement

GCRB is committed to applying the principles of data protection to the processing of personal data at all stages of its lifecycle. The following policy objectives will be adopted:

We will process data fairly and lawfully

- We will only collect personal information where it is necessary so that we can deliver our functions and services;
- We will ensure that if we collect personal data for a specific purpose, or purposes, we will not reuse it for a different purpose that the individual did not agree to or expect;
- We will rely on consent as a condition for processing only where we obtain specific, informed and freely given consent that is affirmative and documented.

We will inform data subjects how their personal data is processed

GCRB will use a privacy notice to let data subjects know what is done with their personal data. This will be published on the GCRB website and available to staff, Board members, visitors and others before collecting and processing their data.

Any processing of personal data beyond the scope of the standard privacy notice will require a separate privacy notice.

Privacy notices will be regularly reviewed and GCRB will inform the relevant data subjects of any changes that may affect them.

Privacy notices will explain, in simple terms:

- What data is collected and why
- The lawful basis we rely on to process the data (for each purpose)
- Whether we use it for any other legitimate purpose
- Whether the data is needed to meet a statutory or contractual requirement
- The source of the data where we receive it from third parties
- Whether we use automated decision making or profiling

- How we will protect the data
- Who we may disclose the data to
- How long we keep the data for and how we dispose of it when no longer required
- How data subjects can update the personal data we hold
- How data subjects can exercise their rights
- Who our Data Protection Officer is and how they can be contacted

We will uphold a Data Subject's rights

GCRB will uphold a data subject's rights to:

- obtain a copy of the information comprising their personal data (known as making a subject access 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.

Subject access requests (requests for a copy of one's own personal data) will be responded to by the college, free of charge, within one month of the request being received. A further two months to respond may be granted in exceptional circumstances, for example if the request is complex or a number of requests are received from the same person.

GCRB will also ensure it communicates to all data subjects their right to lodge a complaint with the Information Commissioner's Office.

We will hold data securely and only for as long as needed to meet the purpose

GCRB has a Data Retention Schedule [1]which applies to all records created, received or maintained by GCRB in the course of carrying out their duties. GCRB has arrangements in place with the Glasgow Colleges, where Glasgow Clyde College for HR and finance purposes (for example paying salaries and remuneration), and City of Glasgow College provide financial processing, accommodation and IT infrastructure.

Each College has in place policies, procedures and guidance relating to data protection, including a Data Retention Schedule to ensure data is only held for the minimum period necessary to meet the

[1] A data retention schedule is being put in place, as at 17.09.19.

purpose for which it was collected. Further details can be found in GCRB's Privacy Notice as to how this data is processed and by which College.

GCRB and the Colleges have stringent security standards in place for the management of personal data, Information Security and Acceptable Use Policies in place that outline steps that must be taken to prevent unauthorised access to personal, special category data and confidential information, limiting any risks associated with the processing of personal data. Each College also provides data protection training to staff to support this.

We will protect the integrity and confidentiality of personal data

GCRB, and in instances where the Colleges processing data on their behalf, will take all necessary steps to reduce the likelihood of data breaches and to reduce the impact of any incidents involving personal data should they occur.

All data breaches will be reported to the Data Protection Officer in the first instance. If a breach is likely to result in a risk to the rights and freedoms of a data subject, the Data Protection Officer will liaise with the Information Commissioner's Office within 72 hours of identifying the breach (in line with legal requirements).

GCRB and the Glasgow Colleges are committed to a culture which encourages early identification of incidents relating to personal data and provide appropriate training and support to individuals involved. Notwithstanding this, GCRB and the Glasgow Colleges will, where deliberate or wilful behaviour leads to a data protection incident, take appropriate disciplinary action and/or report the matter to the police, in line with relevant HR policies.

GCRB and the Glasgow Colleges will also identify 'near misses' where an unplanned event did not lead to a data protection breach but had the potential to. These events will be logged and used as 'learning points' as part of the continual improvement of our data handling processes.

Policy statement on processing of special category and criminal conviction data

GCRB processes special category and criminal conviction data as part of its statutory duties under employment and social protection law (GDPR Article 9(2)(b)). For example, GCRB must process special category data in relation to employment (Schedule 1, Part 1(1) and substantial public interest, specifically 'Statutory etc and government purposes' (for example, reporting on public appointments) and to ensure 'Equality of opportunity or treatment' (Schedule 1, Part 2(6) and (8) respectively, Data Protection Act 2018).

Related policies

This policy has been formulated within the context of the following GCRB documents (and corresponding documents across the Glasgow Colleges):

1. Privacy Notice
2. Data Breach Management Procedure
3. Subject Access Request (SAR) Procedure
4. Data Subject Request Procedure
5. Data Retention Schedule
6. Data Protection Impact Assessment Procedure

7. Freedom of Information Policy Statement
8. Record of Processing Activity (Article 30 ROPA)
9. Data Protection Logs (Breach, SAR, DPIA)