GCRB Glasgow Colleges' Regional Board

Audit Committee Meeting

Date of Meeting	Tuesday 2 October 2018
Paper Title	GDPR
Agenda Item	16
Paper Number	AC1-L
Responsible Officer	Jim Godfrey, Finance & Resources Director
Status	Disclosable
Action	For information

1. Report Purpose

1.1. Note the progress report re GDPR.

2. Recommendations

2.1 The Committee is invited to **note** the report.

3. Evaluation of GDPR

3.1. GDPR is an important issue for GCRB and all three colleges in Glasgow and for GCRB. Previous reports have outlined progress in respect of GDPR and the collaborative approach to Data Protection.

3.2. Members will be aware that Mairead Wood was appointed as the (Shared) Data Protection Officer in May 2018. Over recent months Mairead has been working with the three colleges, and GCRB, to review the arrangements for GDPR and identify areas for improvement.

3.3. An initial report has been prepared and is attached as an annex to this document. The report is welcomed by the Executive Team and the recommendations agreed. The Executive Team is working to incorporate the recommendations into the operational work plan. This plan will include the responsibilities and timescales for implementation.

3.4. A follow-up report, reviewing progress against the actions, will be reported to the Audit Committee at its meeting in March 2019.

4. Risk Analysis

4.1. The approach outlined above enables GCRB, and the Glasgow Region, to address the risks posed by the new regulations in respect of Data Protection and GDPR. In particular, the risk that "There is a breach of legislation/guidance/code of practice and this results in a failure of governance".

5. Equalities Implications

5.1. There are no equalities implications as a direct result of this report.

6. Legal Implications

6.1. The duties and responsibilities in respect of GDPR are detailed in the relevant legislation. Failure to comply with the legislation, relating to GDPR, carries significant financial consequences.

7. Resource Implications

7.1. The primary cost associated with the implementation of the report's recommendations is the cost of staff time.

8. Strategic Plan Implications

8.1. Compliance with relevant legislation is clearly an obligation for GCRB. Whilst GDPR creates an additional administrative burden this is offset by some benefits that might contribute to the achievement of the region's ambitions. Such benefits may include; improved learner confidence and enhanced cyber security.

GDPR DATA PROTECTION COMPLIANCE

GLASGOW CITY REGIONAL BOARD

1. Overview

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. The Board'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 their functions, GCRB have a small team of staff (<5) that are required to collect and process data for the purposes of:

1. Employment (HR) purposes in relation to staffing GCRB and recruiting Board Members under contractual obligation;
2. Complaints including personal data of complainant;
3. Administration of funds from the Scottish Government to its Colleges under legal obligation;
4. Reporting to the Scottish Government (via the Scottish Funding Council) on the administration of funds, including forecasting and monitoring of College spend under legal obligation.

The Post 16 Education (Scotland) Act 2013 underpins the establishment of GCRB and creates the legislative gateway for data sharing.

GCRB is located within the City of Glasgow College's City Campus at 190 Cathedral Street, Glasgow, G4 0RF and shares the same computer network facilities. Data protection and cyber security policies should therefore be aligned to ensure consistency and limit any potential breach risks. However, the size and scale of the College in relation to GCRB are significant. It is therefore advisable that GCRB have their own suite of data protection policies and procedures that are proportionate and tailored to their needs.

2. Requirements under Data Protection Legislation

GCRB is subject to 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.

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).

3. Scope

This report considers the data processing requirements of GCRB in its entirety (i.e. not just personal data) and in relation to its constitution as underpinned by the Post 16 Education (Scotland) Act 2013. This includes the lawful basis for processing, types of data being processed, where this processing takes

place, IT infrastructure, responsibilities of staff, potential risks of processing the data and proposed mitigations and solutions.

The report contains a series of recommendations in relation to policies and procedures that would support GCRB in meeting its data protection obligations going forward.

4. High-Level Data Inventory for GCRB

To understand the data protection needs of GCRB, the data that GCRB processes needs to be fully considered. Below is a high-level data inventory (or information asset register) that has been used to produce this report.

Business Area	Type of Data	Personal Data	Special Category Data	Lawful Basis
a) HR/ Recruitment/ Employment*	CV's, references	Name, address/contact details, etc	Medical notes (e.g. for sickness absence); Trade Union information;	Contractual (Article 6 (1)b GDPR for Personal Data; Employment purposes (Article 9 (2)b for Special Category Data)
b) Administration of funds**	High-level financial allocation (no bank details)	-	-	Legal obligation (Article 6 (1) c)***
c) Reporting	High-level reporting to Scottish Government (SFC)	-	-	Official authority vested in controller (Article 6(1) e)***

** recruitment into GCRB (including CV's, references, etc). Personal data, unlikely to be sensitive personal. Very high-level reporting using aggregate anonymised data.*

*** financial management (i.e. have set allocation of funding to split between 3 colleges, then inform SFC of amount, SFC then make the payment). Have information before it is made public - confidential non-personal data.*

**** non-personal data.*

As can be seen, so long as financial and reporting data being received and processed by GCRB is non-personal data (i.e. anonymised/aggregate data), personal data (potentially including special category 'sensitive' data), should only be processed in relation to staffing (including Board Members) of GCRB.

5. High-level Risk Analysis

The following risk analysis was undertaken based on a number of assumptions identified using the high level GCRB data inventory (see 4).

Assumption	Risk	Mitigation/Solution	Result

1. Personal and special category personal data only contained within HR/Employment business function of GCRB	Unauthorised access results in data breach and could result in a high risk of adversely affecting individuals' rights and freedoms.	- Secure electronic/paper files appropriately - limit access to files on need-to-know basis; - address in data retention schedule	Reduced
2. Board Members receive copies of potentially sensitive/confidential information that may contain personal data	- Board Member (intentionally or otherwise) discloses personal data and/or confidential information	- Only share the minimum data necessary (especially in relation to personal data); -only share personal data for the purpose for which it was collected; - include Members in Data Protection Policy/Privacy Notice/etc; - make Members aware of their responsibilities under GDPR/data protection (this could be written into their contract of employment/as cover note to papers/etc; - request confirmation from Members that Board papers are returned/deleted/destroyed in-line with Data Retention Policy/schedule; - make Members accountable for any data breach.	Reduced
3. Personal data is shared in relation to the reporting/ forecasting business function (NB: personal data is not currently shared for this purpose).	- Data breach (e.g. accidental disclosure of personal data)	- Use anonymised data (i.e.no personal data should be shared) - formalise data sharing arrangements with College's (so if personal data is shared and a breach occurs, procedures are in place to deal with this).	Eliminated

4. Personal data is shared in relation to the financial business function (NB: personal data is not shared for this purpose)	- Data breach (e.g. accidental disclosure of personal data)	- Use anonymised data (i.e.no personal data should be shared) - formalise data sharing arrangements with College's (so if personal data is shared and a breach occurs, procedures are in place to deal with this).	Eliminated
5. Data is not shared in a timely manner by the College's to GCRB	- GCRB cannot meet its legal obligations	- formalise data sharing arrangements	Reduced
6. Remote working results in data being held out with GCRB office (e.g. working from home)	- remote device is misplaced/lost/stolen resulting in data breach	- Establish data protection policy that addresses remote working (e.g. no personal data is saved locally, etc)	Reduced
7. GCRB is based onsite and uses the network of City of Glasgow College.	- GCRB are potentially exposed to any malicious attacks directed towards City of Glasgow College (and vice versa)	- request assurance from CGC regarding storage/hosting of GCRB data, etc.	Accept

Personal and/or special category 'sensitive' personal data is present within the HR/Employment business function of GCRB which may also be shared with Board Members under certain circumstances (e.g. recruitment process) and *may be* accessed remotely. Risks associated with this can be mitigated against to reduce likelihood and consequence of a breach.

Sharing of data from Glasgow's Colleges to GCRB and from GCRB to SFC can be de-risked by anonymising data to significantly reduce (potentially eliminate) the consequence of a breach.

6. Responsibilities (to be included in Data Protection Policy)

Most of the data which GCRB processes does not contain personal data. Some of this information may however be confidential and due care should be taken when processing to prevent disclosure. The following responsibilities are based on City of Glasgow College Data Protection Policy as there is overlap in the infrastructure used by both GCRB and CGC:

Personal (and potentially special category 'sensitive') data is used by GCRB in relation to recruitment of staff including Board Members. Given the small size of GCRB, it is recommended that all users of GCRB 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 Robin Ashton robin.ashton@gcrb.ac.uk who will liaise with the DPO, so that appropriate action can be taken to minimise harm; and
- informing GCRB of any changes to the information that they have provided in connection with their employment, for instance, changes of address or bank account details.

The Executive Director of GCRB, has ultimate accountability for GCRB'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.

The Executive Director are responsible for implementing the policy within their business areas, and for adherence by their staff, including:

- 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;
- 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.

The Data Protection Officer is responsible for:

- informing and advising senior managers and GCRB members 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 GCRB;
- advising on data protection impact assessment and monitoring its performance;
- monitoring and reporting on compliance as required;
- ensuring that data sharing agreements with 3rd parties are in place and maintained;
- providing a point of contact for data subjects with regards 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 data processing;

As GCRB share facilities with City of Glasgow College, including IT infrastructure, the Vice Principal Infrastructure, City of Glasgow College 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.

The Head of Estates, City of Glasgow College 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.

(The Director of Human Resources, at Glasgow Clyde College, Glasgow Kelvin College and City of Glasgow College (as part of the shared support from the Glasgow College's to GCRB) is responsible for maintaining relevant human resources policies and procedures, to support compliance with data protection law.

APUC is responsible for ensuring that supply chain due diligence and procurement processes embed information risk and data protection impact assessment and privacy by design.)

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

Recommendations

Based on the high- level assessment documented herein, GCRB should consider and plan the following:

1. Undertake 'audit' to ensure data held by GCRB for reporting purposes does not contain any personal level data. If personal level data exists, cleanse data to remove personal details.
2. Draft a privacy notice (required under GDPR). There is a privacy statement on the GCRB website in relation to its uses e.g. cookies. A full privacy notice is needed, specifically for GCRB employees and why their data is needed and how it is processed. This should outline the rights of the data subject and how these can be exercised.
3. Create an information asset register (i.e. information asset register (IAR)), detailing the data that is held across GCRB, who owns it, where it is located, its purpose, what format it's in, how long its kept for, does it contain personal data, does it contain special category data, if yes, what processing condition(s) are, is it published, who has access to it, when was it last requested under FOI, does it contain any confidential information, does it hold any exemptions, etc. A high-level data inventory has been produced as a starting point (above). A more detailed register will provide the information needed for records management, data subject requests (including access requests), data protection, freedom of information, information security and information risk. An IAR demonstrates compliance with the GDPR and contains the information required under Article 30 - 'records of processing activity'. This should help to identify the conditions for processing personal and/or special category data and ensure they are robust. If consent is used, how it meets the GDPR requirements, how is it recorded, managed, etc needs

to be recorded and managed. Additionally, an IAR will highlight if any 3rd party data processors are used, including cloud-based organisations (highly likely via Office 365 provided by City of Glasgow College) and any transfer of data out of the European Economic Area (EEA).

4. Produce data retention schedule based on IAR. Assess how retention/deletion will be managed.
5. Once the IAR is drafted, consider any additional data protection risks including mitigation of these. A high-level assessment of the risks across GCRB based on earlier discussions has been developed (above) and can be used as a starting point and amended/built-upon. Consideration of mitigation procedures and solutions should be incorporated into any planning or project management processes by GCRB or any risk register or risk management processes by GCRB.
6. Consider the training needs of staff in relation to their roles and responsibilities and handling of data. This can be provided by the DPO. Annual GDPR/data protection training should be established as a minimum.
7. Formalise data sharing relationships with Colleges, to include outline of purpose of data share, the minimum data required to meet the purpose (ensuring this is anonymised), data retention (i.e. how long you keep the data before destroying), data storage (where data is held), frequency of data share, etc.
8. The following policies/procedures should be established:
    a. Data Protection Policy – to include sections on clear desk, remote working and Board Member's responsibilities.
    b. Data Breach Policy, including effective processes to identify, report, manage and resolve any personal data incidents and/or breaches.
    c. Data Subject Request (including Subject Access Request)
    d. FOISA
    e. Data Protection Impact Assessment (including screening questions)
    f. Information Security Policy (this is likely to come (at least in part) from City of Glasgow College given they are responsible for IT infrastructure and building/facilities.

Summary

The end goal would be to have all these recommendations in place and then monitor compliance with data protection policies and regularly review the effectiveness of data handling and security controls going forward.