E

AUDIT COMMITTEE REPORT

Subject: Internal Audit Assignment – Information Governance	**Purpose:** **For Approval** ☒ **For Discussion** ☐ **For Information** ☐
Prepared by: Hazel Robertson, Vice Principal – Finance and Corporate Services	**Date:** 5 May 2020

Purpose: To present the findings of the Information Governance audit.

Linked to Strategic Goal 3: Provide a high quality College experience.

Executive Summary:

The attached report details the work carried out by the College's internal audit service in reviewing the information governance arrangements in place, specifically covering Data Protection and Freedom of Information. The report confirms a strong overall conclusion with one medium and three low level recommendations made. Six areas of good practice were also highlighted.

Recommendation: Committee consider the findings of the report and approve the auditor's findings.

Previous Committee Approvals: n/a

For publication ☒	**For publication with redactions** ☐	**Not for publication** ☐

Wylie+Bisset
Chartered Accountants, Business & Tax Advisers

Borders College

Internal Audit 2019-20

Information Governance
March 2020

Overall Conclusion
Strong

TABLE OF CONTENTS

Section **Page**

1 EXECUTIVE SUMMARY 2
2 BENCHMARKING 9
3 DETAILED RECOMMENDATIONS 10
4 AUDIT ARRANGEMENTS 15
5 KEY PERSONNEL 16

Appendix **Page**

A GRADING STRUCTURE 18
B ASSIGNMENT PLAN 20

The matters raised in this report came to our attention during the course of our audit and are not necessarily a comprehensive statement of all weaknesses that exist or all improvements that might be made.

This report has been prepared solely for the Borders College's individual use and should not be quoted in whole or in part without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any third party.

We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all system weaknesses that may exist. Neither should internal audit be relied upon to identify all circumstances of fraud or irregularity should there be any although our audit procedures are designed so that any material irregularity has a reasonable probability of discovery. Every sound system of control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas that are considered to be of greatest risk and significance.

1 EXECUTIVE SUMMARY

Overview

Purpose of review

The purpose of this review was to consider whether there were appropriate arrangements in place for management of personal data at the College. We reviewed the steps that have been taken to ensure the College is compliant with the General Data Protection Regulation (GDPR) which was introduced in May 2018. We also reviewed the measures in place for the management of Freedom of Information (FOI) requests at the College.

This review was agreed as part of the 2019-2020 Internal Audit Plan.

Scope of review

Our objectives for this review were to ensure:

General Data Protection Regulation

- The College is compliant with the General Data Protection Regulation (GDPR).
- The College has completed actions identified in the action plan in order to ensure compliance.
- The College has documented plans in place to address any remaining areas of non-compliance.
- There is sufficient reporting in place with regards to the progress with achieving GDPR compliance.

Freedom of Information

- The College is complaint with the legislative guidance of the Freedom of Information.

1 EXECUTIVE SUMMARY

- The College is adhering to its policies and procedures for the freedom of information.
- There is sufficient monitoring and reporting arrangements in place regarding Freedom of Information.

Our approach to this assignment took the form of discussion with relevant staff, review of documentation and where appropriate sample testing.

Limitation of scope

There was no limitation of scope.

Background

The College's GDPR guidelines and approach is set out within the Data Protection Policy, which was approved by the Regional Board in June 2018 and due to be reviewed in June 2021. The College's public facing website contains the full privacy notice which sets out the rights and responsibilities for the College. The College is also registered with the ICO, as confirmed by our review of the ICO register. The current registration is valid until May 2020. The Data Protection Officer for the College is registered with the ICO as the College's Data Protection Officer.

The College as a corporate body and legal entity is the data controller under the legislation. Although the Regional Board is ultimately responsible, the College has designated the Vice Principal: Finance & Corporate Services as responsible for the implementation of the Policy. The Vice Principal: Finance & Corporate Services is also the single point of contact in the College. Furthermore, a Data Protection Officer has also been appointed. In order to adhere to the requirements of the General Data Protection Regulation (GDPR); the College set up an action plan, and has developed an "Article 30 Register". This Register is split into the various area/departments of the College. The objective of the Article 30 Register is to satisfy the requirements set out in the GDPR; it can/will be provided to the Information Commissioner on request. The College use this register as a tool to identify where further work is required.

Individual managers of the various departments within the College are responsible for identifying, recording and reviewing any personal data held by their department, both in electronic and paper format. It is their responsibility to verify information to ensure it is accurate and not held beyond a reasonable length of time.

1 EXECUTIVE SUMMARY

The Freedom of Information (Scotland) Act 2002 (FOISA) provides individuals with a right of access to all recorded information held by public bodies. As a result of this, FOISA requires the College to adopt and maintain a publication scheme and to publish information in accordance with the scheme. The Vice Principal: Finance & Corporate Services is responsible for processing and monitoring all Freedom of Information requests received by the College. The College maintain a spreadsheet to record all requests received and the actions taken by the College. For 2019/20, the College has received 19 Freedom of information requests.

Work Undertaken

Our work undertaken for this assignment included the following:

- Discussions with key personnel to establish the current arrangements in place for the management of any personal data held by the College.
- We obtained and reviewed evidence that actions identified in the College's GDPR Action Plan/Article 30 Register were being addressed.
- We obtained and reviewed documented policies and procedures to confirm that they are appropriate, comply with GDPR/Data Protection and reflect current practice. We assessed how staff, students and third parties are made aware of the College's GDPR requirements.
- Discussions with key personal to establish the monitoring arrangements in place to ensure that the College continues to comply with the GDPR requirements. We evaluated these to ensure these are fit for purpose.
- Ascertaining whether the College had a valid ICO registration in place.
- Reviewing the relevant policies and procedures for Freedom of Information process.
- Discussions with the relevant staff members responsible for processing and monitoring Freedom of Information requests.

1 EXECUTIVE SUMMARY

- Reviewing the internal log/spreadsheet which records Freedom of Information requests received by the College.

1 EXECUTIVE SUMMARY

Conclusion

Overall conclusion

Overall Conclusion: Strong

We can provide a strong level of assurance that the College has adequate arrangements in place in relation to information governance. We can also provide a strong level of assurance that the College are complying with requirements for Freedom of Information requests as set out in the relevant act of parliament and recommendations/requirements by the Office of the Scottish Information Commissioner. However, we have raised 4 recommendations for improvement. Please see section 3 for further information.

Summary of recommendations

Grading of recommendations

	High	Medium	Low	Total
Information Governance	0	1	3	4

As can be seen from the above table there were no recommendations made which we have given a grading of high.

Areas of good practice

The following is a list of areas where the College is operating effectively and following good practice.	
1.	The Data Protection Officer and Vice Principal: Finance & Corporate Service have a monthly catch up where they review the Article 30 Register. The Vice Principal: Finance & Corporate Services will also provide a verbal update at the monthly Senior Leadership Team (SLT) meeting.
2.	The College's public facing website clearly guides anyone (staff/student/third party) on the process to follow if/when they want to make a request via the Freedom of Information (Scotland) Act 2002.
3.	The College's ICO registration is valid until 22 May 2020. The Data Protection Officer is noted as the main point of contact.
4.	The Freedom of Information (FOI) procedure outlines that the Vice Principal: Finance & Corporate Services has overall responsibility. All FOI requests are directed to the Vice Principal: Finance & Corporate Services in the first instance. The request will be assessed and then directed to the most appropriate person(s). A log detailing the number of FOI requests is made available on the College's public facing website.
5.	The College reports the Freedom of Information (FOI) requests to the Office of the Scottish Information Commissioner (OSIC) quarterly. The College along with other public bodies are required to provide statistics about the request for information they have received and how they have responded. The College must provide this data to OSIC every 3 months via their statistics portal. Along with the above, we noted FOI data is provided to the Regional Board on an annual basis.

1 EXECUTIVE SUMMARY

The following is a list of areas where the College is operating effectively and following good practice.	
6.	The College also has a Digital Delivery and Development Group (DDG). The DDG includes key managers, the Data Protection Officer, the Vice Principal: Finance & Corporate Services, Student Support, Human Resources and IT Support within the College. The DDG understands how data flows within the College and where weaknesses/potential areas of risk are. The DDGs primary purpose is to ensure that the College are compliant with GDPR. The DDG meet every second month.

2 BENCHMARKING

We include for your reference comparative benchmarking data of the number and ranking of recommendations made for audits of a similar nature in the most recently finished internal audit year.

Information Governance

Benchmarking				
	High	Medium	Low	Total
Average number of recommendations in similar audits	0	2	1	3
Number of recommendations at Borders College	0	1	3	4

From the table above it can be seen that the College has a higher number of recommendations compared to those colleges it has been benchmarked against.

3 DETAILED RECOMMENDATIONS

Article 30 Register			
Ref.	Finding and Risk	Grade	Recommendation
1.	The College maintain an action plan to ensure its continuing compliance with GDPR, which includes the Article 30 Register. The Register is split into different departments to monitor their use of personal data. The Register is maintained by the delegated managers with the support of the Data Protection Officer and reviewed monthly with the Vice Principal: Finance & Corporate Services. During our review, we found that several areas of the Register were blank or had not been updated such as privacy notices and data destruction timeframes. Each department was also required to submit information to the Data Protection Officer however, we were informed that this is still a work in progress. There is the risk that the College will not achieve the expected benefits of the register if this is not being fully utilised. There is also the risk that not all departments within the College are able to evidence their GDPR compliance.	**Medium**	We recommend that the College ensure that the Article 30 Register is fully completed and continues to be monitored monthly.
Management response			Responsibility and implementation date
The majority of departments have created their Article 30 register but some require further refinement. This register meets the Article 30 requirements of GDPR and is a live document, updated as and when processing changes, stops or new processing activity occurs.			*Responsible Officer:* DPO *Implementation Date:* End of June 2020

3 DETAILED RECOMMENDATIONS

Freedom of Information: Policy/Procedure			
Ref.	Finding and Risk	Grade	Recommendation
2.	The College were able to evidence compliance with the Freedom of Information (FOI) legislation and we were provided with a copy of the FOI guide and FOI Procedure for review. During our review, we found that the FOI Procedure has not been updated to reflect the change in personnel for the Vice Principal: Finance & Corporate Services. The Procedure refers to "he" rather than "she. The College could consider gender neutral language such as "they" to resolve any future change in the role. We were also unable to confirm the last review date of the College's Model Publication Scheme. We do note that the current Scheme reflects current practice within the College. We also found that the link on the College's public facing website for FOI "requests made for information under the Freedom of Information from January 2018" does not work. There is the risk that the College are not reviewing and maintaining their FOI documentation.	**Low**	We recommend that the College review the Freedom of Information Procedure and update this were required. The College could consider gender neutral language such as "they" to resolve any future change in the role. We also recommend that the College document its review dates for its Model Publication Scheme. We also recommend that the College review the link on their website for Freedom of Information to ensure this is active and is working as required.

Management response			Responsibility and implementation date
Due to the low level of FOI requests these matters are deemed low risk. These will be progressed by end September by the VP F and CS.			*Responsible Officer:* Vice Principal: Finance & Corporate Services *Implementation Date:* End of September 2020

3 DETAILED RECOMMENDATIONS

Data Protection Champions			
Ref.	Finding and Risk	Grade	Recommendation
3.	The College aim to ensure that there is an individual within every department to provide initial support to the department on any data protection issues. The College created Data Protection Champions as such a support role. The Data Protection Champions are not to act as "mini Data Protection Officers". During our review, we found that Data Protection Champions were being asked to undertake tasks that were outwith their role, such as data protection breach investigations and that they were being held accountable for data protection issues within their department. We do note that the College are aware of this issue and are planning to hold a staff meeting in April 2020 to clearly define the roles, responsibilities and title of the Data Protection Champions. There is the risk that the Data Protection Champions may be requested to undertake tasks normally out with their remit.	Low	We recommend that the role of the Data Protection Champion should be clearly defined and recirculated to staff members.
Management response			Responsibility and implementation date
The role/remit has been agreed by SLT and the HR Development Officer and the DPO are working on additional training and regular network meetings to ensure staff are supported and the risk identified do not occur			*Responsible Officer:* DPO *Implementation Date:* Action complete

3 DETAILED RECOMMENDATIONS

Data Retention/Destruction Policy and Procedure			
Ref.	Finding and Risk	Grade	Recommendation
4.	The College should have a Data Retention Policy and Procedure. The Policy and Procedure should detail the personal data held by the College, their retention period and the procedures for destroying data outwith its retention period. During our review, we found that the College's Data Retention Policy & Procedure was currently in draft format and has yet to be fully implemented and approved by the Board. There is the risk that there is no clear guidance for staff members on data retention and data destruction.	**Low**	We recommend that the College complete the Data Retention Policy and Procedure and that is reviewed and approved by the Board.
Management response			Responsibility and implementation date
The implementation of this action will flow from the Article 30 register and will be enabled by the roll out programme for One Note and Sharepoint.			*Responsible Officer:* Head of ISLT *Implementation Date:* End of September 2020

5 AUDIT ARRANGEMENTS

The table below details the actual dates for our fieldwork and the reporting on the audit area under review. The timescales set out below will enable us to present our final report at the next Audit Committee meeting.

Audit stage	Date
Fieldwork start	9 March 2020
Closing meeting	11 March 2020
Draft report issued	25 March 2020
Receipt of management responses	30 April 2020
Final report issued	30 April 2020
Audit Committee	21 May 2020
Number of audit days	3

6 KEY PERSONNEL

We detail below our staff who undertook the review together with the College staff we spoke to during our review.

Wylie & Bisset LLP			
Partner	Ross McLauchlan	Partner	ross.mclauchlan@wyliebisset.com
Senior Manager	Stephen Pringle	Senior Internal Audit Manager	stephen.pringle@wyliebisset.com
Auditor	Faisal Kayani	Internal Audit Senior	faisal.kayani@wyliebisset.com
Auditor	Siobhan Archibald	Internal Audit Assistant	siobhan.archibald@wyliebisset.com

Borders College			
Key Contact	Hazel Robertson	Vice Principal (Finance and Corporate Services)	hrobertson@borderscollege.ac.uk
Wylie & Bisset appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and co-operation.			

APPENDICES

A GRADING STRUCTURE

For each area of review, we assign a level of assurance in accordance with the following classification:

Assurance	Classification
Strong	Controls satisfactory, no major weaknesses found, no or only minor recommendations identified.
Substantial	Controls largely satisfactory although some weaknesses identified, recommendations for improvement made.
Weak	Controls unsatisfactory and major systems weaknesses identified that require to be addressed immediately.
No	No or very limited controls in place leaving the system open to significant error or abuse, recommendations made require to be implemented immediately.

A GRADING STRUCTURE

For each recommendation we assign a grading either as High, Medium or Low priority depending on the degree of risk assessed as outlined below:

Grading	Classification
High	Major weakness that we consider needs to be brought to the attention of the Audit Committee and addressed by senior management of the College as a matter of urgency.
Medium	Significant issue or weakness which should be addressed by the College as soon as possible.
Low	Minor issue or weakness reported where management may wish to consider our recommendation.

Purpose of review

The purpose of this review is to consider whether there are appropriate arrangements in place for management of personal data at the College. We will review the steps that have been taken to ensure the College is compliant with the General Data Protection Regulation (GDPR) which was introduced in May 2018. We will also review the measures in place for the management of Freedom of Information (FOI) requests at the College.

This review was agreed as part of the 2019-2022 Audit Needs Assessment.

Scope of review

Our objectives for this review are to ensure:

General Data Protection Regulation

- The Association is compliant with the General Data Protection Regulation (GDPR).
- The College has completed actions identified in the action plan in order to ensure compliance.
- The College has documented plans in place to address any remaining areas of non-compliance.
- There is sufficient reporting in place with regards to the progress with achieving GDPR compliance.

Freedom of Information

- The College is complaint with the legislative guidance of the Freedom of Information.
- The College is adhering to its policies and procedures for the freedom of information.

- There is sufficient monitoring and reporting arrangements in place regarding Freedom of Information.

Our approach to this assignment took the form of discussion with relevant staff, review of documentation and where appropriate sample testing.

Limitation of scope

There is no limitation of scope.

Audit approach

Our approach to the review will be:

General Data Protection Regulation

- Discussion with key personnel to discuss the current arrangements in place for the management of any personal data held by the College.
- Review of documented policies and procedures to confirm that they are appropriate, comply with the Data Protection Act and reflect current practice.
- Physical verification of the controls in place to mitigate the risk of loss, misuse or theft of personal data.
- Where relevant sample testing to confirm that processes are operating as expected.

Freedom of Information

- Discussion with key personnel to discuss the arrangements in place for the management of Freedom of Information requirements.
- Review of documented policies and procedures to confirm that they are appropriate, comply with Freedom of Information requirements.

- Obtaining evidence that actions identified in the College's Action Plan are being addressed.

Potential key risks

The potential key risks associated with the area under review are:

- The College is not compliant with the General Data Protection Regulation (GDPR).
- The College has not completed the actions identified on their Action Plan in order to achieve compliance.
- The College does not have documented plans in place to address remaining areas of non-compliance.
- There is insufficient reporting in place regarding the progress towards GDPR compliance.
- There is a risk that the College are not following guidance that is set out on the freedom of information act.
- There is a risk that the College are not adhering to their policies and procedures for freedom of information.
- The Association are not registered with a ICO.
- There is insufficient monitoring arrangements in place.
- There is insufficient reporting arrangements in place regarding Freedom of information.