Board of Management
Audit Committee

Date: 19 February 2019 **Time: 2pm** **Room: 2009**

A G E N D A

			Presented by
1	Welcome and Apologies		HC
2	Declaration of Interest		HC
3	Minute of Meeting of 13 November 2018	(attached)	HC
4	Matters Arising not on the Agenda		HC
	4.1 Feedback from Recommendations to the Board • External Audit Report and Financial Statements for 2017-18	(verbal)	BJ
	4.2 Board Toolkit, five questions from the National Cyber Security Centre	(verbal)	AW
5	Internal Audit Contract – Tender update	(attached)	KH
6	GDPR & Cyber Security		
	6.1 GDPR Policy	(attached)	AG
	6.2 Cyber Security Update	(attached)	AG
7	Whistle Blowing Policy	(attached)	CT
8	Anti-Fraud & Corruption Policy	(attached)	KH
9	Risk Management Policy	(attached)	CT
10	*Internal Audit Reports		
	10.1 Action Tracking Spreadsheet	(attached)	KH
	10.2 Progress Report	(attached)	PC
11	Audit Scotland		
	11.1 Audit Scotland letter on the fees for 2018-19	(attached)	KH
	11.2 Upcoming Feedback Request re: External Audit	(attached)	KH
12	Strategic Risk Register	(attached)	CT
13	Any Other Business		
14	Date and Time of Next Meeting – Tuesday, 7 May 2019 at 2pm		

*Individual Internal audits reports are not published on the website; they are included in the published annual internal audit report

Board of Management-Audit Committee

Minute of the Meeting of the Audit Committee of the Board of Management of Dumfries and Galloway College held on 19 February 2019 at 2 pm in Room 1074b

Present:	Hugh Carr (Chair)	Robbie Thomas (via Facetime)
	Pat Kirby	
In attendance:	Carol Turnbull	Andy Glen (Vice Principal)
	Karen Hunter, Head of Finance	Ann Walsh (Board Secretary)
	Katy Matkin (RSM) (via telephone) – for agenda no 10.2 only	
Minute Taker	Heather Tinning (Executive Assistant)	

1 Welcome and Apologies

The Chair welcomed all to the meeting. Apologies for absence were intimated on behalf of Stuart Martin and Naomi Johnson. Katy Matkin (RSM) attended the meeting by teleconference on behalf of Philip Church (RSM).

The Board Secretary confirmed the meeting was quorate.

2 Declaration of Interest

Members agreed to indicate declarations of interest as appropriate throughout the meeting.

3 Minute of Meeting of 13 November 2018

The Minute of the meeting of 13 November 2018 was approved.

4 Matter Arising not on the Agenda

4.1 Feedback from recommendations to the Board (External Audit Report and Financial Statements for 2017-18)

The Chair reported that these had been given unqualified approval.

4.2 Board Toolkit, five questions from the National Cyber Security Centre

The Board Secretary advised that an update would be provided at the next meeting.

5 Internal Audit Contract – Tender Update

The Head of Finance spoke to the report which had been issued, reporting on key points, including:

- The APUC framework had been refreshed – members noted the eight Contracts
- In terms of the period, the Head of Finance suggested a 3 year followed by a 2-year period, allowing to refresh after 3 years if necessary. The last appointment was 5 years

The committee also discussed the Evaluation Criteria and agreed the following amendment:

- 70% Quality /30% Price – replacing 60%/40% as suggested in the report

The committee also agreed:

- Audit Approach – 10% - instead of 7.5% as suggested in the report
- Quality Assurance – 10% - instead of 7.5% as suggested in the report
- Audit Procedures – 10% - instead of 5% as suggested in the report

Following a request, the Head of Finance advised that the Evaluation of Tender responses due on 2nd May would be shared with the committee. The responses are due in on 30th April.

Members reviewed the proposed procurement timetable, service requirements, and the evaluation criteria, and suggested changes were agreed.

Decision: The Committee agreed the proposed contract period of 3 years followed by a 24-month period of extension where agreed by both parties

Actions:

- The Head of Finance to make necessary changes as agreed
- The Head of Finance to share a summary report of the Evaluation Tender Responses with the committee for input

6 GDPR & Cyber Security

6.1 GDPR Policy

The Vice Principal Business Development & Corporate Services spoke to the report that had been issued, reporting that the draft GDPR Policy had been revised following advice from the Colleges' Shared Data Protection Officer, Lisa Powell. The key change includes the roles of the key staff members. The papers presented to the committee include the Updated Policy and Data Breach Procedure for formal approval. The Vice Principal reported that over 92% of staff have completed online GDPR Training and advised that staff are fully compliant of GDPR. Members welcomed the updated policy. The Vice Principal confirmed that periodically test processes are in place throughout the course of the year for both GDPR and Cyber Security.

Members approved the Data Protection Policy.

6.2 Cyber Security Update

The Vice Principal Business Development & Corporate Services spoke to the report, reporting that the college successfully gained Cyber Essentials in April 2018, and are working towards re-certifying for Cyber Essentials in April 2019. The ICT Manager is compiling a Operational Plan for completion in the summer. In terms of the ICT works, Windows 7 is end of life on 14 January 2020 and the ICT team are in the process of upgrading the remaining Windows 7 PCs, as part of a planned spend. In terms of security, the Vice Principal confirmed that the Network Drives are backed up on a daily basis as part of a secure back up for all college data.

Action: The Vice Principal Business Development & Corporate Services to report back to members whether the security camera is connected to the college internet system

Members noted the report and agreed to continue to monitor Cyber Security activities.

7 Whistle Blowing Policy

The Principal spoke to the report which had been issued, updating members on the changes to the Whistle Blowing Policy. The Policy originally was under the remit of the Vice Principal Business Development and Corporate Services and has now been remitted to sit with the Head of HR. Following current practice, the recent changes include:

- Change in the title to include Public Interest Disclosure to reflect the change in terminology more widely used currently
- Change of responsibility to Head of Human Resources to reflect the new structure and remits of posts in the college
- Additional undertaking of the college to protect all parties involved in the process
- Additional links to the disciplinary procedure for false or malicious allegations

The Principal reported that both the previous and the revised policy had been included for member's comparison. With regard to the information on the Public Domain the Principal confirmed that there is no relation to the Whistle Blowing Policy.

Decision: Members approved with minor amendment
Action: The Policy to be amended as agreed:

- Section 5.1 to read: Abuse of this policy by staff making 'knowingly' false or malicious allegations

8 Anti-Fraud & Corruption Policy

The Head of Finance spoke to the report which had been issued, providing an overview of the changes to the Anti-Fraud & Corruption Policy. Minor changes have been made to the previous policy, including an update on code of good governance to Scotland's Colleges.

Members reviewed the changes and recommended the revised Policy to the Board.
Action: Financial Regulations update to be presented to the next committee meeting

9 Risk Management Policy

The Principal spoke to the report which had been issued, providing members with an updated Risk Management Policy. The Principal advised that both the previous and the current Policy had been included for comparison and comment. Following discussion on point 5.7 in terms of the threshold that has not been included in the revised policy, it was agreed not to include this but to look at each threshold on its own merit.

Members reviewed and approved the updated Risk Management Policy.

10 *Internal Audit Reports

10.1 Action Tracking Spreadsheet

The Head of Finance spoke to the Action Tracking Spreadsheet, highlighting key points:

- The actions have been reviewed by the Internal Auditors, subject to change at the next review
- Actions are on track to meet deadlines
- Four actions in progress as at beginning of February

In terms of risk 12 (Health and Safety), the Principal advised that the H&S Committee would consider any risks of concern. A H&S report is presented to the College Leadership Team, and will also be presented to the HR Committee in October. In terms of the number of incidents reported at the last Audit Committee meeting, the VP BDCS advised that following recent training, staff are more aware of reporting H&S incidents.

Members noted the Action Tracking Spreadsheet.

10.2 Progress Report

Katy Matkin, Assistant Manager, (RSM) joined the meeting by teleconference, on behalf of Philip Church (RSM), presenting the Progress Report, a summary of assurance giving the college an update on progress against the 2018/19 plan.

In terms of the summary update on progress members noted:

- 43% - complete
- 14% - plan in draft, a report has been issued to college Management
- 29% - plan in progress, draft report to follow

- 14% - Final report in plan
    - On 8th April an Audit of Final Planning and Forecasting will take place

Katy advised that the remaining four Audits will be presented to the next committee meeting in May. Overall, members noted that the college is on track to achieve.

Members noted the Report.

11 Audit Scotland

11.1 Audit Scotland letter on the fees for 2018-19

The Head of Finance spoke to the Audit Scotland letter received on their proposed fee update. She advised that Scott Moncrieff are still to confirm their fee which will be included in their Audit Plan.

11.2 Upcoming feedback request re: External Audit

The Head of Finance spoke to the report which had been issued, advising that Audit Scotland are proposing to issue a Questionnaire on the work of the External Auditors, which will be on online version. Members requested confirmation on who would be asked to complete the survey.

Action: The Head of Finance to check if a college response is required and confirm with members

12 Strategic Risk Register

The Principal spoke to the Strategic Risk Register, reporting on the recent changes, including:

- Risk No 2.6 – Failure to achieve credit targets
- Risk No 2.7 – Insufficient Student Support Funding to meet Demand
- Risk No 3.5 - Industrial Relations Problems
- Risk No 3.9 – Failure to reach Aspirational Standards in learning, teaching and service delivery

Members approved the Strategic Risk Register

13 Any other Business

The Chair asked to formally note that Stuart Martin was leaving the Audit Committee and recognised his time as a member of the Committee. Also, the Principal is leaving the college in February, and wished Carol well in her new Post.

14 Date and time of Next Meeting

The next meeting of the Audit committee is to take place on Tuesday 7 May 2019 at 2 pm.

Board of Management-Audit Committee

Minute of the Meeting of the Audit Committee of the Board of Management of Dumfries and Galloway College held on 13 November 2018 at 2 pm in Room 1074b

Present:	Hugh Carr (Chair) Naomi Johnson	Robbie Thomas (via facetime)
In attendance:	Carol Turnbull Karen Hunter, Head of Finance Philip Church (RSM)	Andy Glen (Vice Principal) Brian Johnstone (Regional Chair) Claire Gardiner (Scott-Moncrieff)
Minute Taker	Heather Tinning (Executive Assistant)	

1 Welcome and Apologies

The Chair welcomed all to the meeting. Apologies were intimated on behalf of Stuart Martin, Pat Kirby and Ann Walsh (Board Secretary).

The Chair confirmed the meeting was quorate.

The Chair brought the confidential agenda item forward for discussion with the Auditors, asking that the college staff leave the meeting at this point.

2 Good Governance – Confidential discussion (without college staff)

The Chair invited Philip Church to feedback to the committee on any issues or concerns that RSM wished to draw to the committee's attention. Philip spoke positively of the relationship between Internal Audit and Management, and stated there were no issues or concerns to report to the committee. He spoke positively of the standard of controls tested and reviewed by Internal Audit, and of the approach taken to implementing recommendations made, noting that this gave an encouraging view of the overall standard of control and governance in the college.

(The college staff were invited to return to the meeting)
(Claire Gardiner joined the meeting following the Confidential discussion)

3 Internal Audit Report

3.1 Health & Safety

Philip Church spoke to the report, highlighting key points:

- The Head of Corporate Services has now been appointed with overall responsibility for Health & Safety in the college
- There have been 60 Health & Safety incidents reported, between period January 2018 to October 2018
- Detailed findings highlighted two medium priorities, including:
  - A lack of upward reporting of Health and Safety statistics, ie Annual Health & Safety Report to the Board
  - Weaknesses identified in terms of additional training needs with regards to staff using machinery and equipment where there may be additional safety training required
- Two low priority findings include:

- Concerns with roles and responsibilities for reporting under RIDDOR had not been clearly documented
- There had been no recent Health & Safety Committee meetings owing to recent internal restructures. A new Health & Safety Committee, who are responsible for the monitoring of incidents, to form and meet quarterly, no later than January 2019.

Philip Church reported overall a reasonable assurance opinion.

3.2 Progress Report

Philip Church reported on the Progress Report, advising that this is a standing agenda item, which gives the committee assurance on how the college is performing. Progress against the 2018/19 internal audit plan, approved by the committee on 17 May 2018, highlights 43% of assignments were complete. The KPIs against the internal audit plan have been achieved.

Members noted the report.

Philip Church left the meeting.

4 Declaration of Interest

Members agreed to indicate declarations of interest as appropriate throughout the meeting.

5 Minute of Meeting of 19 September 2018

The Minute of the meeting of 19 September 2018 was approved.

6 Matters Arising

6.1 Revised GDPR Policy Update-latest draft

The Vice Principal Business Development & Corporate Services reported that the Audit Committee approved the Interim Data Protection Policy on 18th May 2018. Lisa Powell, the Data Protection Officer (DPO), is based at Dumfries College campus on a regular basis and has met with key college staff to consider the GDPR Policy. The draft policy, yet to include named personnel, will be brought back to the committee following completion. The DPO reported that the restructured document is in line with that of colleges across the sector, and also reported on other documents including:

- The draft Subject Access Requests Procedure - requests to be responded to within one calendar month
- The Data Breach Procedure - a working document

The DPO reported on her overall role, as an advisory responsibility, rather than an operational responsibility. The DPO advised of the importance of staff training and awareness as key for the college, including demonstrating compliance, records of processing activities and records of consent. Data Security responsibilities and Practices of sharing papers to be brought to the Board for discussion. The Principal advised that Board papers are uploaded to AdminControl, a secure programme, to allow members to access these and reported that sharing of papers/documents through e-mails would be looked at moving forward to ensure the college remains compliant and secure with sending documents externally.

Members thanked the Data Protection Officer for the update.

6.2 Data Breach Procedure - draft

The Data Protection Officer advised that the draft Data Breach Procedure was developed as a template, which is used across the college sector. Any data security incidents have to be highlighted and assessed for risk. The DPO advised the timescale of 72 hours from when the breach has been

identified. Following discussion, the DPO advised that there is no legal requirement to report to the SFC. The college has an appointed person with operational responsibility to notify the DPO immediately should there be a breach.

Members thanked the Data Protection Officer for the update.

7 External Audit Annual Report

Claire Gardiner spoke to the External Audit Annual Report from Scott Moncrieff, which concludes the audit work for 2017/18. Points were discussed at the recent clearance meeting and actions agreed. The annual accounts will be presented for approval at the Board meeting on 11 December 2018. In terms of financial sustainability, the Principal advised that the College Leadership Team are holding a Strategic meeting in December to look at future finances and Curriculum Planning for 2019/20. A number of measures are in place at present. Three risks highlighted, including:

- Documentation of Journal Authorisation – Implementation date 30 November 2018
- UWS Scotland Contract – Implementation date 31 December 2018
- Financial regulations and authorised signatory listing – Implementation date 31 March 2019

Claire Gardiner thanked the Head of Finance and the Finance Team for their help and support.

8 2017-18 Draft Financial Statements

The Head of Finance spoke to the report, highlighting key points to note:

- Scott Moncrieff had provided an unqualified Audit opinion to include in the accounts
- A revised comment has been included in the notes on depreciation cash spend
- Movement between forecast breakeven and underlying deficit has been detailed in the accounts
- There is an approximate deficit of £74,000
- Income and Expenditure not fully known until year end
- In terms of the SOSEP Project, balance to be added to the accounts following formal offer of grant

The Principal reported on the £74,000 deficit, which was owing to matters arising around the year-end, including:

- Timing of drawing down FWDF income
- Technical note received in terms of payment as part of National Bargaining for TQFE
- Single Sick/Holiday pay for member of staff

The Head of Finance reported that a paper will be presented to the Finance & General Purposes Committee on 20 November, to inform of changes made in the processes to the budget scrutiny.

The Chair thanked the Head of Finance and asked for a formal note to be recorded to the Head of Finance and the Finance Team.

9 Internal Audit Contract

The current contract with RSM was extended for one-year, with a view to tendering via the APUC framework for a new contract starting on 2019-20. The framework has been refreshed, and a number of new forms are now on the list of preferred suppliers, including RSM. The college will be able to run a mini-competition using the framework rather than having to go to full tender.

Action: The Head of Finance to draft a tender paper, and gather input on questions for the evaluation and scoring from the Committee

Members noted the report

10 Action Tracking Sheet/GDPR Actions

The Head of Finance reported that the actions highlighted in the External Audit Report and the Health and Safety Report have been added to the tracker, advising that the College Leadership Team also discuss the action tracking sheet on a monthly basis. Members noted that most actions are on track for completion in terms of GDPR.

11 Scott-Moncrieff's Non-Executive Directors Forum on Risk

Robbie Thomas reported on the Non-Executive Directors Forum that he attended. There were various discussions including Cyber Security, Brexit and Assurance Mapping. Robbie spoke of the Board Toolkit, five questions from the National Cyber Security Centre to be shared with Board Members, including:

- How do we defend our organisation against phishing attacks?
- How does our organisation control the use of privileged IT accounts?
- How do we ensure that our software and devices are up to date?
- How do we make sure our partners and suppliers protect the information we share with them?
- What authentication methods are used to control access to systems and data?

Action: The Board Secretary to take the Toolkit forward with Board Members - https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda

Members noted the report.

12 Strategic Risk Register

The Principal spoke to the Strategic Risk Register, advising that the Risk Register is presented and discussed at monthly College Leadership Team meetings to allow for wider discussions. Members noted the three changes to the recent Register including:

- Risk No 3.5 – Industrial Relations Problems
  - Likelihood increased to 5
- Risk No 3.11 – Failure to meet the SOSEP funded project deadlines
  - New Risk
- Risk No 3.12 – Failure to reach contractual agreement with CITB regarding delivery of Construction Related Apprenticeship
  - New Risk

The Principal confirmed that all controls are in place.

Members approved the Strategic Risk Register

13 Any other Business

None.

14 Date and time of Next Meeting

The next meeting of the Audit committee is to take place on Tuesday 19 February 2019 at 2 pm.

Audit Committee

TENDER FOR THE COLLEGE INTERNAL AUDIT CONTRACT

1. Purpose of the Report

1.1 The purpose of this report is to provide an outline of the proposal for the procurement plan for the College Internal Audit Contract, and ask for the Committee's input for the evaluation criteria and other aspects of the tender.

1.2 Advance Procurement for Universities and Colleges (APUC) have established a Framework Agreement for internal audit services. The Framework is split into four lots – Internal Audit - large, Internal, Audit – Small, External Audit and Tax. Lot 2, Internal Audit - Small – has eight contractors:

BDO
Scott Moncrieff
Wylie & Bissett
RSM
TIAA Ltd
Henderson Loggie
KPMG
Mazars

1.3 As Scott Moncrieff currently act as External Auditors to the College, the Invitation to Tender (ITT) will not be sent to them.

1.4 The APUC Framework allows the College to undertake a mini-competition in order to appoint a contractor, which will be more efficient and straightforward to undertake than implementing a full tender exercise, and is still fully compliant with the relevant procurement regulations.

1.5 The combined technical and Commercial scores for the top 5 contractors are higher than 80%, which indicates that the tender responses were very high quality.

2. Key dates

2.1 The proposed timetable for this procurement exercise is as follows:

Draft timetable and evaluation criteria to be reviewed by Audit Committee	Tuesday 19 February 2019
Tender Issued	Friday 12 April 2019
Tender Return	Midday Tuesday 30 April 2019
Evaluation of Tender Responses	Thursday 2 May 2019

Audit Committee

Award Date	Friday 10 May 2019
Service Commences	Wednesday 01 August 2019

2.2 The proposed timetable above allows for consideration of the evaluation by the Audit Committee at their next meeting, and allows some flexibility in the timing of the tender evaluation.

3. Service requirements

3.1 The tender papers will set out in detail a full specification of the audit requirements.

3.2 The proposed contract period is for three years from 1August 2019, with an option to extend for a further 24 months where both parties agree to do so.

3.3 The scope of the internal audit contract is based on the current service, and will cover all of the College's activities, and reporting structure as well as potentially special investigations or reviews requested by the Board.

3.4 The annual audit of Student Support Funds and Further Educational Statistical (FES) Return is proposed to be included in the scope of the tender, and KPI's will be considered as part of the contract management.

3.5 The proposed pricing schedule requests a daily rate, partner/manager/qualified and other staff split, and an estimated number of days required for the work under the contract, together with any other charges which may be made under the contract.

4. Evaluation criteria

3.1 The draft evaluation criteria for the ITT is as follows:

	Weighting	Award Criteria	Sub-weighting
Price	**40%**		**40%**
Quality	**60%**		
		Management Structure	**10%**
		Audit Experience	**10%**

		Audit Cycle – plan and responsibilities	**10%**
		Sample Reports	**5%**
		Audit Approach	**7.5%**
		Quality assurance	**7.5%**
		Audit Procedures	**5%**
		Range of Specialist expertise	**5%**

3.2 The evaluation questions will be tailored to request sufficient information for each of the evaluation criteria sub-headings in order to score the responses appropriately.

5. Recommendation

Members are asked to review the proposed procurement timetable, service requirements, and the evaluation criteria, and suggest any changes.

Audit Committee

DATA PROTECTION POLICY AND DATA BREACH PROCEDURE

Due to changes to the European Union General Data Protection Regulation ("GDPR"), the UK Data Protection Act 2018 ("DPA 2018") and other relevant legislation protecting privacy rights, the College has reviewed the above policy and procedure to ensure compliance.

The College holds personal information on a variety of data subjects including students - past and present, staff, customers, suppliers and members of the public. As a Data Controller we have obligations to fulfil whilst holding, transferring and processing and protecting this information.

The Data Protection Policy outlines how the College will fulfil its obligations and provides guidance to ensure all those responsible for handling and processing data are aware of their roles and follow a common and consistent approach. This Policy applies to all locations from which College data is accessed, including home and overseas.

The Principal has ultimate accountability for the College's compliance with data protection law. In line with our responsibilities as a Data Controller, we have appointed a designated Data Protection Officer (DPO). The DPO provides guidance and support to the College in fulfilling its obligations under Data Protection Law. The DPO can be contacted at dpo@dumgal.ac.uk.

DATA BREACH PROCEDURE

Article 4 of the GDPR defines a personal data breach as:

'A breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.'

Due to the amount of data the College processes and stores, we need to ensure we have a robust and systematic process for handling data breaches to ensure we can act legally, responsibly and timely. There can be many reasons for data breaches, whether it be accidental or malicious and as technology develops, there are new ways for how data can be breached and it is important that the College has a rigorous process for monitoring systems and practises.

Any data security breach can have serious consequences for the College, including loss of reputation, legal claims, substantial sanctions including suspension of processing and potential fines of up to £18 million.

The College contacts for data breaches are:

Data Protection Officer: Lisa Powell
Senior Contact: Andy Glen, Vice Principal
Operational Contact: Lorraine Grierson, Central Admin Support Manager
Head of ICT: Calum Rodgers.

Audit Committee

This Procedure outlines the College's commitment and response to any data breach, ensuring that they are logged and managed in accordance with the law and best practice.

This Procedure should be read alongside the Data Protection Policy.

Lorraine Grierson
Central Admin Support Manager, 11/2/19

DATA PROTECTION POLICY

Contents

1. Introduction

This Policy outlines how Dumfries and Galloway College ("the College") will fulfil its obligations as a Data Controller and where applicable, a Data Processor, under current legislative provisions for data protection, including the EU General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 ("DPA 2018") and such guidance as may be issued by the UK Information Commissioner.

2. Purpose

The purpose and benefits of this policy are to raise awareness of the College's data protection arrangements to ensure that a common and consistent approach is adopted in relation to the management of information and the protection of personal data in order that:

- Information is collected, processed, held, transferred and disposed of appropriately;
- Staff are aware of their rights and responsibilities in relation to information handling;
- Appropriate mechanisms are in place to ensure that individuals whose personal information the College hold, are advised of their rights.

3. Policy Statement

In undertaking the business of the College, we create, gather, store and process large amounts of data on a variety of data subjects (individuals) including students (potential, current and former), staff, customers / suppliers and members of the public. This includes personal and special categories of personal data, which are subject to data protection laws.

With the ability to collect and process data comes a responsibility to ensure that this is collected, used and stored appropriately. The College must, therefore, ensure that data is managed in line with relevant legislation and guidance and that those involved in data handling and processing are aware of their responsibilities.

The College is committed to applying the principles of data protection and other requirements of data protection law to the management of all personal data at all stages of its lifecycle.

4. Scope

This policy applies to:

- All data created or received in the course of college business in all formats, of any age. "Data" shall include personal and special category data; and also confidential and commercially sensitive data;
- Data held or transmitted in physical (including paper) and electronic formats;
- Data transmitted in verbal format (e.g. in conversation, in a meeting, or over the telephone).

Who is affected by the policy?

- College staff (which includes contractors, temporary staff and anyone else who can access or use data, including personal and special categories of data, in their work for the college);
- Non-staff data subjects (these include, but are not confined to): prospective applicants; applicants to programmes and posts; current and former students; alumni; former employees; family members where emergency or next of kin contacts are held, members of the Board of Management and the College committees, volunteers, potential and actual donors, customers, people making requests for information or enquiries, complainants, professional contacts and representatives of funders, partners and contractors.

Where the policy applies:

- This policy applies to all locations from which college data is accessed, including home use and overseas.

5. Responsibilities

All users of college information (staff, students, volunteers and other users) are responsible for:

- Completing relevant training and awareness activities provided by the College to support compliance with this Data Protection Policy and other relevant procedures;
- Taking all necessary steps to ensure that no breaches of information security result from their actions;
- Reporting all suspected information security (data) breaches or incidents promptly so that appropriate action can be taken to minimise harm;
- Informing the college of any changes to the information that they have provided in connection with their studies or employment, for instance, changes of address or bank account details.

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

The Vice Principal Business Development & Corporate Services is responsible for:

- Acting as the contact for the Executive Team and ensuring that the College and staff comply with Data Protection legislation;
- Reporting to the Principal, the Audit Committee, Board of Management, and Executive Team on relevant risks and issues.

The **Head of Corporate Services** is responsible for:

- Ensuring the security of all centrally managed IT systems and services operated by the College and the protection of electronic data;
- Promoting good practice in IT security among staff;
- Ensuring that IT security risks related to data protection are captured on the College risk registers;
- Ensuring that controls are in place to manage the physical security of the College, including CCTV, taking account of relevant data protection laws and risks.

The Head of Human Resources (HR) is responsible for:

- Maintaining relevant HR policies and procedures to support compliance with data protection law;
- Ensuring that staff roles and responsibilities are clearly defined in terms of data protection and that staff contracts reflect this.

The Head of Academic Planning and Quality is responsible for:

- Maintaining relevant student administration policies and procedures;
- Oversight of the management of student records and associated personal data across the College in compliance with data protection law.

The designated College Officer with operational responsibility for Data Protection is responsible for:

- Managing internal data protection activities and ensuring that procedures are in place for individuals to exercise any of their rights;
- Working with the DPO and senior managers to develop and implement appropriate data protection policies and procedures.

The Data Protection Officer (DPO) 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 supporting 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 Team, the Board of Managers and committees as appropriate;
- Ensuring that Records of Processing and Third 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;

- Monitoring personal data breaches, and recommending actions to reduce their impact and likelihood of recurrence;
- Acting as the contact point for and cooperating with the Information Commissioner's Office (ICO) on issues relating to processing.

Where permissible under the legislation, some of these duties may also be undertaken by the designated College Officer with operational responsibility for data protection.

All Heads of Services are responsible for:

- Promoting a culture of data protection compliance across the College and within their area of responsibility;
- Implementing the policy in their Faculty or Service, and for adherence by their staff;
- Ensuring that those processing data in their roles are supported in doing so appropriately.

All Team Managers are responsible for implementing this policy within their business areas and for adherence by 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 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 IT staff to put in place equivalent IT security controls;
- Assisting the designated College Officer with operational responsibility for data protection, and the DPO , in maintaining accurate and up to date records of data processing activities;
- Ensuring that they and their staff cooperate and support the designated College Officer with operational responsibility for data protection, and the DPO , in relation to subject access requests and other requests relating to personal data where the data is managed by their business area;
- Recording data protection and information security risks on the Organisational Risk Register and escalating these as necessary.

As part of the College's internal audit programme, the Audit Committee will instruct the College's Internal Auditors to audit the management of personal information, data protection risks and the College's compliance with relevant data protection laws.

6. Data Protection Principles

Under data protection laws the College is responsible for, and must be able to demonstrate compliance with the six data protection principles under the GDPR.

The College will ensure that all data processing for which it is responsible is conducted in line with these principles and this policy documents how this will be achieved in practice.

Principle 1: Personal data shall be processed fairly, lawfully and transparently

This means that the College will:

- Only collect and use personal data in accordance when we have a lawful basis to do so (see section 7, Lawful Basis for Processing);
- Treat people fairly by using their personal data for specific purposes and in a way that they would reasonably expect;
- Rely on consent, as the legal basis for processing, only where we obtain specific, informed and freely given consent, that is affirmative and documented; and can be easily withdrawn at any time.

Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation').

This means that the College will:

- ensure that if we collect personal data for one purpose (e.g. to provide advice on study skills), we will not reuse this 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);
- inform data subjects about the specific purposes of processing and tell them what we are doing with their personal data.

Principle 3: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

This means that the College will:

- Only collect personal information where it is necessary so that we can deliver our functions and services;
- Reduce risks of disclosure by anonymising personal data wherever necessary, (e.g. when using it for statistical purposes), so that individuals can no longer be identified;
- Review the data we hold and where appropriate delete what we do not need.

Principle 4: **Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').**

This means that the College will:

- Take all reasonable steps to ensure the personal data we hold is accurate and record the source of that data (e.g. from data subject or partner organisation);
- Have processes in place to ensure that incorrect data is rectified or erased as soon as possible;
- Update personal data where appropriate, (e.g. when informed of a change of address our records will be updated accordingly).

Principle 5: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation');

This means that the College will:

- Only keep personal data for as long as necessary for the purpose it was collected for; and destroy records securely in a manner appropriate to their format;
- Apply agreed retention periods to all records containing personal data;
- Have appropriate processes in place to comply with individuals' requests for erasure under the 'right to be forgotten'.

Principle 6: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

This means that the College will:

- Have robust organisational measures in place to protect personal data, including physical and technical security measures (e.g. secure rooms and storage where appropriate, an ICT Security Policy and ICT Acceptable Use Policy;
- Control access to personal data so that staff, contractors and other people working in the College can only see the personal data that 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 data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles;
- Implement a Data Breach Procedure to manage, investigate and, where applicable, report security incidents to the ICO and data subjects affected.

The Accountability Principle

Accountability is central to GDPR. The College must take responsibility for what it does with personal data and how it complies with the above principles.

The College is required to maintain necessary documentation of all processing activities; implement appropriate security measures (technical and organisational); perform Data Protection Impact Assessments (DPIAs) and designate a DPO.

7. Lawful Basis for Processing

To be able to process personal data lawfully, the College must ensure that all processing falls within one or more of the lawful bases (conditions for processing) as set out in Article 6 of the GDPR. These are:

- **Consent** – An individual has provided clear consent for the processing of their personal data for one or more specified purposes;
- **Contract** – The processing of the personal data is necessary to fulfil a contract that the College has with an individual;
- **Legal Obligation** – Processing of data is necessary to comply with the law, other than to fulfil a contractual reason;
- **Vital Interests** – Processing of data is necessary to protect someone's life;
- **Public Task** – Processing is necessary for the College to perform a public interest task or to fulfil its official functions, where the task or function has a clear legal basis;
- **Legitimate Interests** – Processing is necessary for the College's legitimate interests or the legitimate interests of a third party, unless the need to protect an individual's personal data overrides those legitimate interests.

At each point that the College collects data, the lawful basis for processing will be made clear.

8. Privacy notices

The College will use privacy notices to let data subjects know what is done with their personal data. The text of all privacy notices will be consistent across the College and will confirm what the lawful basis is for the processing of the data.

Privacy notices are published on the college website and are made available to individuals from their first point of contact with the College.

Any processing of staff or student data beyond the scope of the standard privacy notices will mean that a separate privacy notice is required.

We will regularly review these privacy notices and will inform the data subjects of any changes that may affect them.

9. Data Subjects Rights and Subject Access Requests

Data subjects have the following rights under data protection law:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

These rights are explained in further detail in Appendix 2, ‘Guide to Data Subjects Rights’.

The College will uphold Data Subject Rights (DSRs) and have appropriate processes and procedures in place to ensure these rights can be actioned if an individual makes a request. It is important to note that some rights have certain conditions that must be met for the rights to apply.

Individuals always have the right to request access to their personal data that the College holds (known as making a Subject Access Request (SAR). Any data subject may make such a request and receive a copy of their information usually free of charge and within one month of their request. For further details see ‘Guide - How to make a Subject Access Request’ and ‘Subject Access Request Procedure’.

When an individual makes any request to exercise any of their rights then the designated College Officer with operational responsibility for data protection must be informed immediately, so this can be recorded and processed accordingly. **All requests must be answered within one month.**

The College will maintain a central DSR Register to demonstrate for audit and reporting purposes that we are meeting the deadlines for handling all requests. The DSR Register will be held securely by the designated College Officer with operational responsibility for data protection.

The College will also ensure it communicates to all data subjects their right to lodge a complaint with the ICO.

10. Data Protection Impact Assessments (DPIAs)

Where the College proposes to introduce or amend new systems or working practices that have implications for its data protection arrangements, a DPIA will be completed to assess these implications, manage risk and to consider what control

measures are appropriate to ensure that data remains protected and all processing remains compliant with the principles set out above.

Where any relevant new project or system is being considered the DPO must be advised at the earliest opportunity in order that they can consider the proposal and determine whether a Data Protection Impact Assessment is required. For further information please contact the DPO via the data protection mailbox dpo@dumgal.ac.uk.

11. Staff Training

The College will provide initial data protection training for all staff (existing and new), with additional specialist training given to staff in areas with specific responsibilities for processing personal data and sensitive information. Periodic refresher training will be given to all staff.

Completion of initial and refresher training in data protection will be mandatory for all College staff.

12. Data Sharing

In the performance of its duties in relation to the employment of staff and the services provided to learners, the College is required to share information with external organisations. Example bodies with whom the College may be required to share or give access to data include:

Scottish Government	Scottish Funding Council
Awarding Bodies	Education Scotland
Skills Development Scotland	HMRC
Pension Funds	Trades Unions
Local Authorities	Insurance Companies
Legal Advisers	Scottish Public Services Ombudsman
Auditors	Suppliers of services, such as College systems

In all such cases where personal data is shared externally, the College will ensure that appropriate safeguards are in place through agreed protocols or data sharing agreements by College Officer with operational responsibility for data protection.

12.1 Transfer of Data / Information Cross Campus

College staff may only share the personal data we hold with another member of staff if the recipient has a job-related need to know. Most data processed by the College is available via relevant College systems at any campus to those who require access and there should be no need for such data to be transferred by staff using portable means. (For further information about the use of USBs, portable hard drives and the transfer of manual files see Section 13, Data Security and the ICT Security Policy / Housekeeping Guidance).

12.2 Data Sharing with the Police and Statutory Agencies

There is a particular exemption within the data protection legislation relating to requests for access to personal information received from the police, law enforcement agencies and other bodies with statutory functions to detect or prevent crime. Such requests should normally be made in writing and signed by someone of sufficient authority within the agency requiring the information. (Will insert link once uploaded)

If you receive a request from such an agency, you must consult with a member of the Executive Management Team who will make the decision whether personal information should be released.

12.3 Disclosure of data to third parties

The College must ensure that personal data is not disclosed to unauthorised third parties which includes family members. All staff and students should exercise caution when asked to disclose personal data held about an individual to a third party. Disclosure must be relevant to, and necessary for, the conduct of College business.

Requests for information in relation to an individual will only be accepted if produced in writing, on company-headed paper. The reason for making the request and, where appropriate, the legal basis for the request must be detailed. Where appropriate, a statement from the data subject consenting to disclosure to the third party should accompany the request.

If there is any doubt as to whether it is legitimate to disclose personal information to a third party, staff should seek advice from their line manager who will consult with the designated College Officer with operational responsibility for data protection, a member of the Executive Management Team, or the DPO as necessary.

13. Data security

The following general principles apply at all times to all data managed by the College, whether the data are personal and/or special category data; confidential business data; or commercially sensitive data:

- All college users of data must ensure that all data, and specifically personal and special category data, they hold is kept securely;
- Users must ensure data is not disclosed to any unauthorised third party in any form either accidentally or otherwise (including verbal disclosure);
- Desks should be left clear at the end of each working day; paperwork shall be locked away when not in use;
- Portable devices (laptops, memory sticks, external hard drives) should not be left unattended.

For further information see ICT Security Policy/Housekeeping Guidance.

14. Data retention and disposal

The College will develop a College wide Data Retention Schedule**.** This sets out the basis on which information can be retained and documents retention periods; as set out in legislation or in line record keeping requirements set by relevant statutory bodies.

Personal data must only be kept for the specified retention period. Once information is no longer needed it should be disposed of securely.

The College has appropriate measures in place for the deletion and disposal of personal data. Manual records are shredded and disposed of as "confidential waste" and arrangements are in place to permanently erase the hard drives of redundant electronic equipment.

15. Data Breaches

While the purpose of this policy is to ensure that the College's data protection arrangements are effective and well understood, it is also important to recognise the behaviours and actions that would be considered as breaches of the policy and the consequences of any such breach. The following occurrences are considered breaches of this policy:

- Unlawful procurement of information by anyone not entitled to access such information;
- Unfair processing i.e. processing information for a purpose other than that for which it was provided;
- Processing of inaccurate information, particularly if information was known to be inaccurate or steps could have been taken to ensure accuracy;
- Unlawful disclosure i.e. sharing of information with anyone not entitled to receive it or loss of any data subject to this policy;
- Collection, storage or processing of inadequate, irrelevant or excessive information.

The College will take all necessary steps to reduce the likelihood of Personal Data Breaches and to reduce the impact of any incidents involving personal data that do occur.

In line with the College's Data Breach Procedure all personal data breaches (suspected and actual) must be reported your Line Manager and the designated College Officer with operational responsibility for data protection immediately. If a breach is likely to result in a risk to the rights and freedoms of an individual, the DPO must be informed as the College is required to report to the ICO within 72 hours of notification.

The College will record all data incidents and reportable breaches. We will use these events as 'learning points' as part of the continual improvement of our data handling processes.

The College is committed to a culture which encourages early identification of personal data incidents and which provides appropriate training and support to individuals involved. However, the College 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.

16. Risks of non-compliance

The penalties for a breach of the GDPR are significant. This may include penalties of up to €20m or 4% of global annual turnover for the most serious breaches of the law; plus claims for compensation and damage to reputation.

Misuse of personal data, through loss, disclosure or failure to comply with the data protection principles and the rights of data subjects, may result in significant legal, financial and reputational damage for the College.

Non-compliance with the data protection principles, or any concerns over data protection, must immediately be reported to dpo@dumgal.ac.uk and to your Line Manager.

17. Monitoring and review

The College will review its practices and guidance on a regular basis to ensure that they reflect our commitment to ensuring fair, consistent and lawful management of data. This policy will be reviewed every three years to reflect legislative requirements, recommendations and identified good practice.

18. Linked Policies/Related Documents

This policy should be read in conjunction with the College's:

- ICT Security Policy
- ICT Acceptable Use Policy
- Data Breach Procedure
- Subject Access Request Procedure
- Guidance note – How to make a Subject Access Request
- Data Security Policy / Housekeeping Guidance
- Disciplinary Policies and Procedures
- Links to documents:
    - https://intranet.dumgal.ac.uk/adminnet/applications/docs/index_nav.aspx?sec=130
    - https://intranet.dumgal.ac.uk/adminnet/applications/docs/index_nav.aspx?sort=1&sec=131&sd=0

19. Distribution

- All Staff
- Quality Manual

Contents

1 BACKGROUND

1.1 Dumfries and Galloway College ("the College") needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act legally and responsibly, and protect personal data, which it processes. Data security breaches are increasingly common occurrences whether caused through human error or malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached.

1.2 Any data security incident may have serious consequences for the College, including reputational damage, legal claims as well as substantial sanctions involving orders to suspend processing and potential fines of up to £18 million.

1.3 Under the General Data Protection Legislation ("GDPR"), the College must report a significant data breach to the Information Commissioner's Office ("ICO") within **72 hours** of becoming aware of it. This procedure outlines the actions needed to identify if a breach has taken place, how to manage the breach and how to record, and if necessary report a breach.

2 AIM

2.1 The aim of this procedure is to standardise the College's response to any data breach and ensure that incidents are appropriately logged and managed in accordance with the law and best practice, so that:

- incidents are reported swiftly and can be properly investigated
- incidents are identified as a breach where appropriate and handled accordingly
- incidents are dealt with in a timely manner and normal operations restored
- incidents are recorded and documented
- the impact is understood, and action taken to prevent further damage
- the ICO and data subjects are informed in more serious cases
- incidents are reviewed, and lessons learned.

3 DEFINITION

3.1 For the purpose of this procedure an incident is any suspected Personal Data Breach.

3.2 Article 4 (12) of the GDPR defines a Personal Data Breach as:
"a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

3.3 The College is obliged under the GDPR to act in respect of such data incidents and breaches. This procedure sets out how the College will manage a report of a suspected Personal Data Breach. The aim is to ensure that where personal data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the

incident is properly investigated and reported, and any necessary action is taken to rectify the situation.

3.4 A Personal Data Breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy
- Data posted, emailed or faxed to the incorrect recipient
- Loss or theft of equipment on which data is stored
- Inappropriate sharing or dissemination of data whether accidental or malicious
- Staff accessing information to which they are not entitled
- Hacking, malware, data corruption
- Information is obtained by deception or “blagging”
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data.

3.5 In any situation where staff are uncertain whether an incident constitutes a Personal Data Breach, please report it to the Central Administration Manager and the Data Protection Officer (DPO) will be informed immediately. If there are IT issues, such as the security of the network being compromised, ICT should be informed immediately.

3.6 Contacts:

- DPO: Lisa Powell, DPO@dumgal.ac.uk.
- Senior Management Contact: Andy Glen, Vice Principal Planning and Performance, glena@dumgal.ac.uk, 01387 734005
- Operational Contact for Data Protection: Lorraine Grierson, Central Administration Manager, griersonl@dumgal.ac.uk, 01387 734364
- Head of ICT: Calum Rodgers, Head of ICT, rodgersc@dumgal.ac.uk, 01387 734245

4 SCOPE

4.1 This college-wide policy applies to all College information, regardless of format, and is applicable to all staff, students, visitors, contractors, partner organisations and data processors acting on behalf of the College. It is to be read in conjunction with the College Data Protection Policy document, which is available on the College’s website.

5 RESPONSIBILITIES

5.1 Information users

5.1.1 The GDPR applies to both Data Controllers (the College itself) and to those acting on behalf of the College as Data Handlers. Therefore, all information users are responsible for reporting actual, suspected, threatened or potential Personal Data

Breaches and / or security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

5.1.2 It is everyone's responsibility to report incidents. If you identify an actual incident (which includes any data security breach) or if you are concerned that one may have occurred, then you must report it immediately whether within or outside office hours (i.e. on a 24 x7 basis).

5.2 Managers

5.2.1 Heads of Department are responsible for ensuring that staff in their area act in compliance with this procedure and assist with investigations as required.

5.2.2 Where a Personal Data Breach is suspected the Senior Manager for Data Protection, the DPO, the Head of Department (where the breach has occurred), the College Officer with operational responsibility for Data Protection and appropriate members of the College's Executive Management Team (EMT) will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. This group will be known as the Data Breach Response Team. Suitable further delegation may be appropriate in some circumstances

6 REPORTING A BREACH

6.1 Internal

6.1.1 Suspected Personal Data Breaches should be reported promptly to the Senior Manager for Data Protection AND to the College Officer with operational responsibility for Data Protection. The DPO will then be informed immediately as the primary contact. Individuals reporting a breach must also inform their Line Manager. The report must contain full and accurate details of the incident including:

- Who is reporting the incident?
- When it happened?
- What classification of data is involved?
- The scale of the breach including the number of individuals it may affect.

6.1.2 The incident report form should be completed as part of the reporting process. Appendix 1.

6.1.3 Once a data incident has been reported an initial assessment will be made to establish whether it is a Personal Data Breach, and the severity of the breach. Appendix 2. This will be used to inform the College's decision about whether the breach is reportable to the ICO.

6.1.4 All personal data security incidents will be centrally logged by the DPO to ensure appropriate oversight in the types and frequency of confirmed incidents. The DPO is also responsible for monitoring and reporting to EMT / SMT as required.

6.1.5 A Personal Data Breach may also occur within an organisation that handles information on the College's behalf (data processors). Such organisations are required to notify the College of a Personal Data Breach without undue delay. If you are notified of a suspected Personal Data Breach by an external organisation, you must report it immediately using the same reporting procedure detailed in 6.1.1

6.2 External

6.2.1 Article 33 of the GDPR requires the College as data controller to notify the ICO only when the breach "is likely to result in a risk to the freedoms and rights of natural persons". Notification must be made "without undue delay" and within 72 hours of the College becoming aware of the breach. If the College fails to do this, it must explain the reason for the delay.

6.2.2 Article 33(5) requires that the College must maintain documentation on data breaches, their nature and remedial action taken.

6.2.3 A report to the ICO must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of DPO, likely consequences of the breach and action taken.

6.3 Method of notification

6.3.1 Notifiable breaches are to be reported to the ICO by telephone or online. Notifications may only be made by the DPO as the primary point of contact.

7 DATA BREACH MANAGEMENT PLAN

7.1 The College's response to any reported Personal Data Breach will involve the following four elements:

- Containment and Recovery
- Assessment of Risks
- Consideration of Further Notification
- Evaluation and Response

7.2 Each of these four elements will need to be conducted in accordance with the data breach flowchart Appendix 3. An activity log recording the timeline of the incident management should also be completed.

7.3 Containment – take appropriate steps to identify the nature and extent of the Incident (whether the Incident is a Personal Data Breach) and contain the Incident, including establishing who needs to be made aware of the Incident and inform them what they are expected to do to assist in the containment exercise.

7.4 Recovery – assess whether any information lost can be recovered and what steps (if any) can be taken to limit the damage or harm that may have been caused.

7.5 Assessment of Risks - assess the Incident in terms of its type, severity and risk according to the criteria described in Appendix 2.

7.6 Consideration of Further Notification may involve the following:

- Notification of individuals
- Notification to controllers
- Other notifications

7.7 Notification to individuals

7.7.1 In addition to the requirement to notify the ICO, Data Protection Law requires organisations to communicate Personal Data Breaches to the affected individual data subjects where the risk assessment is that the likely risk to the individuals is high. Please note that the threshold for communicating Personal Data Breaches to individuals is higher than the threshold for notifying the ICO. It is therefore possible that there may be a legal obligation to notify the Regulator but not communicate with affected individual data subjects.

7.7.2 Even where the risk is not high, the College may nevertheless choose to notify individuals of the Personal Data Breach. The decision to notify or not is a matter for the Incident Response Team, who will take account of the facts and circumstances of the Personal Data Breach.

7.7.3 Timing - Data Protection Law provides that communication with individuals should happen 'without undue delay'. The expectation is that any communication should be made as soon as reasonably feasible and in close co-operation with the ICO and other relevant bodies e.g. law enforcement agencies. The exact timing of any communication may depend on its purpose. If the communication is to help individuals avoid immediate risk of further detriment, then it should be made promptly. Advice and guidance on how to avoid similar breaches in future may be communicated at a later date.

7.7.4 Content – Data Protection Law prescribes the minimum content for the communication to individuals. It must include:

- a description of the nature of the breach
- the name and contact details of the DPO or other contact point
- a description of the likely consequences of the breach
- a description of the measures taken or proposed to be taken by the organisation to address the breach, including, where appropriate, measures to mitigate its possible adverse effects. This might include advice regarding change of passwords etc.

7.7.5 Any communication should be specific to the Personal Data Breach. It should not, for example, include any marketing or other general content.

7.7.6 Method of communication – Any communication should be made directly to data subjects unless to do so would involve disproportionate effort, in which case a public message (e.g. on the College website or twitter) will be used to communicate the Personal Data Breach to individuals. Several channels of communication may need to be employed to maximise the chances of reaching all affected individuals. The College's Marketing Team should be involved where public notification is required to ensure the College is effectively managing the situation from a customer relations perspective.

7.8 Notification to Controllers

7.8.1 Where the College is a Joint Controller or an Independent Controller in a relationship (for example with the Scottish Funding Council) the College must notify the other Controller of the Personal Data Breach without undue delay. Data Protection Law does not specify what information must be provided to the Controller, but the Data Sharing Agreement will set out specific details for breach notification.

7.8.2 Where the College acts as a Processor and processes personal data on behalf of another organisation (the Controller) the College must notify the Controller of the breach without undue delay. Data Protection Law does not specify what information must be provided to the Controller, but the contract between the College and the Controller may set our specific contractual obligations. Where the College acts as a Processor the College does not have an obligation to notify either the Regulator or the affected individuals. The Controller is responsible for determining whether the Personal Data Breach must be notified to the Regulator and the affected individuals.

7.9 Other notifications

7.9.1 It may be appropriate to communicate the occurrence of Personal Data Breaches to other appropriate bodies. These may include:

- Law Enforcement Agencies - notifying an incident to law enforcement agencies if any of the conduct concerned may have involved criminal activity
- Insurers – the College may choose to notify its insurers of a breach. It is important that any incident is notified to them promptly if the relevant insurance is to respond.

7.9.2 Any recommendation as to whether to notify any of these bodies should be identified in the initial report provided by the Team investigating the incident

7.10 Evaluation and Response - following the reporting of a Personal Data Breach the College will evaluate the effectiveness of the response. The College will make/recommend any adjustments/improvement to this Policy, any related policies and guidance or any systems or processes and procedures to address any issues identified. The College will also identify any future corrective actions and assess the effectiveness of any corrective actions that have been implemented.

7.11 An incident will only be closed once all of the issues identified in responding to the incident have been addressed and all corrective actions have been taken and completed.

8 DISCIPLINARY

8.1 Staff, students, contractors, visitors, partner organisations, data processors and board members who act in breach of College policy and procedure may be subject to disciplinary procedures or other appropriate sanctions.

9 FURTHER INFORMATION / GUIDANCE AND REFERENCES

- The GDPR https://gdpr-info.eu/
- ICO GUIDANCE ON DATA BREACHES https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

10 ASSOCIATED DOCUMENTS

10.1 The following policies should be read in conjunction with the Data Breach Procedure:

- Data Protection Policy (currently under review)
- Information Security Policy

11 LEGISLATION

11.1 Legislation relevant to this policy includes:

- The General Data Protection Regulation (EU) 2016/679
- The Data Protection Act 2018

13 MONITORING AND REVIEW

13.1 This document shall be formally reviewed by January 2022.

Appendix 1: Data Security Incident Reporting Form

	Report By:	Name: Job Title: Department: Date:
1.	Summary of event and circumstances	Who, what, when, etc. How did you become aware of the breach? When did it happen?
2.	Type and amount of personal data	Type - what information has been compromised? Include title of documents and categories of personal data. For a list of categories use checklist below. Amount – How many personal data records have been compromised? AND How many data subjects are affected?
3.	Action taken	Include action taken by the person who discovered the breach and any action taken by the person reporting to the DPO (e.g. to investigate the incident)
4.	Action taken to retrieve data and respond to incident	
5.	Procedure/policy in place to minimise risk	For example, College Data Protection Policy and Guidance, Information Security Policy, existing contract / data sharing agreement
6.	Breach of policy/procedure?	Has there been a breach of College policy or local procedure and has appropriate management action been taken?
7.	Complaint received?	Have you received any communication from any of the data subject(s) about this incident?

8.	Details of Data Protection training	Date of most recent training by staff involved

DPO TO COMPLETE THIS SECTION

9.	Further information requested	Y / N	DPO signature Date
10.	Report completed	Y / N	DPO signature Date

Categories of personal data included in the breach (please tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade Union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☐ Basic personal identifiers e.g. name, contact details
- ☐ Identification data e.g. usernames, passwords
- ☐ Economic and financial data e.g. credit card number, bank details
- ☐ Official documents e.g. driving licences
- ☐ Location data
- ☐ Genetic or biometric data
- ☐ Criminal convictions or offences
- ☐ Not yet known
- ☐ Other (please give details)

Appendix 2 – Risk Assessment Matrix

DATA SUBJECTS AFFECTED

Description	Scenario	Code Letter	Risk Rating Value
Very High	1000+	VH	5
High	500-999	H	4
Medium	100-499	M	3
Low	10-100	L	2
Very Low	0-10	VL	1

IMPACT

Description	Score	Code Letter	Risk Rating Value
Very High	Individuals may encounter very significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).	VH	5
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).	H	4
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).	M	3
Low	Individuals may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).	L	2
Very Low	No evidence that individuals will be materially affected.	VL	1

SEVERITY

Score = DATA SUBJECTS AFFECTED SCORE X IMPACT SCORE

Description	Score	Notify ICO	Notify Data Subjects
Very High	20+	Yes	Yes
High	16-19	Yes	Consider
Medium	11-15	Consider	Consider
Low	6-10	No	No
Very Low	1-5	No	No

The overall matrix will be used to assess the severity of the incident and inform the decision on whether to notify the ICO and data subjects. A final decision about notification to ICO, and whether to inform the data subjects will be made by the Data Breach Response Team.

RECORD OF DECISION (to be completed on behalf of the Data Breach Response team)

- Risk rating score – VL / L / M / H
- Notify ICO – Y/N
- Notify Data subjects – Y/N
- Other notification – insert details

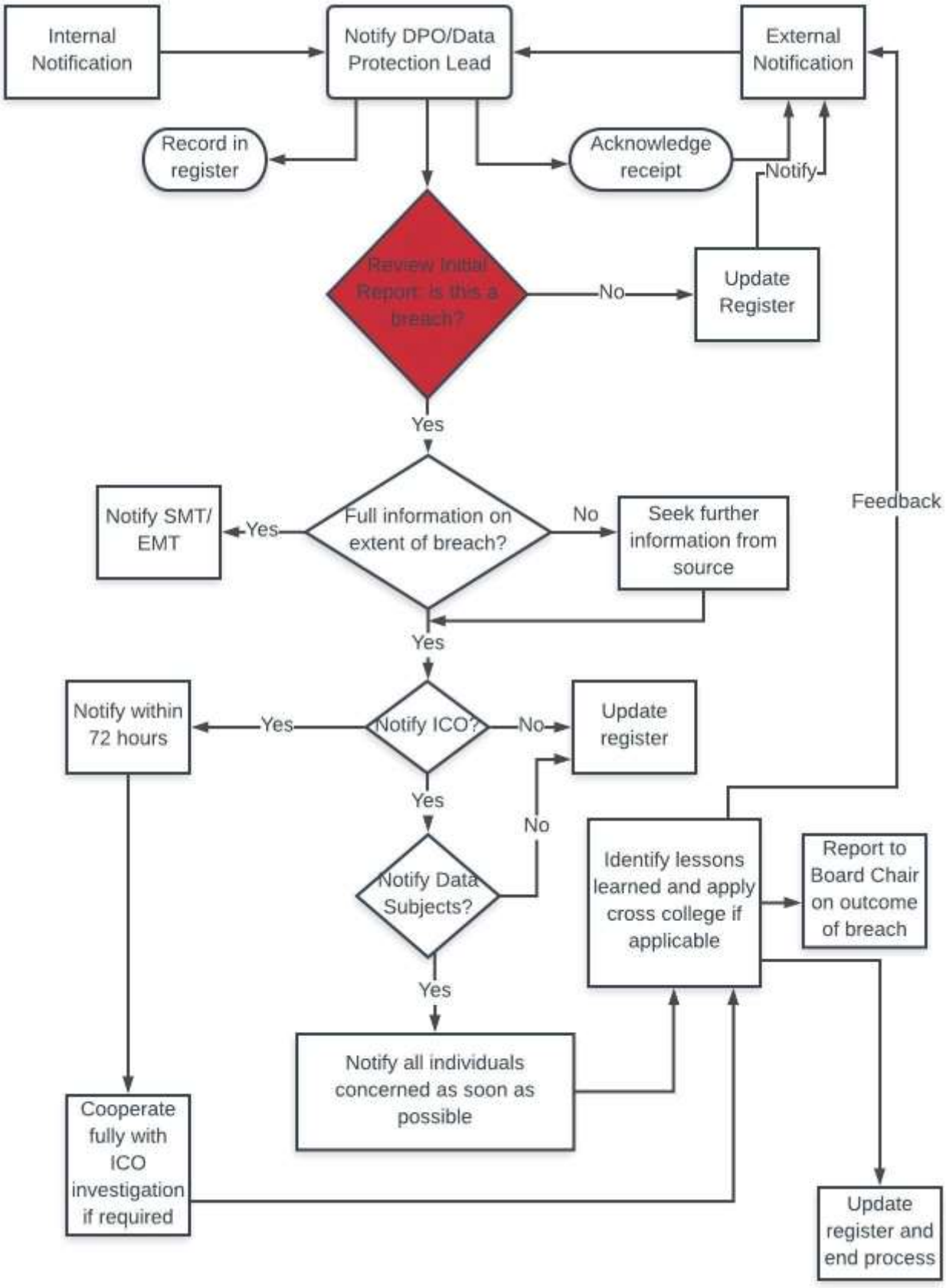
Signed by:
Andy Glen, Senior Manager for Data Protection

Date:

Signed by:
Lisa Powell, Data Protection Officer

Date:

Appendix Three: Data Breach Flowchart



Audit Committee

Cyber Security Update

1 Purpose of the Report

The purpose of this report is to provide the Audit Committee with an update on Cyber Security.

2 Cyber Security Update

The College are due to re-certify for Cyber Essentials in April so are working towards obtaining this again. It is currently planned to go for Cyber Essentials Plus in the following 12 months.

Windows 7 is end of life on 14th January 2020, so the ICT department are in the process of upgrading the remaining Windows 7 PCs. The team plan to upgrade the hard drives to solid state ones and add additional RAM to improve performance. It is planned to have this completed before the start of the next academic year.

The ICT Manager has been working with the Chief Information Security Officer (CISO) from Higher Education Further Education Shared Technology and Information Services (HEFESTIS) to come up with an incident response plan in relation to cyber security. It is hoped to have this plan completed in the next couple of months.

Through HEFESTIS the Head of Corporate Services and the ICT Manager now have direct access to current and emerging threats including online forum access to discuss possible and actual threats with other institutions.

It is hoped that awareness tools can be developed and rolled out to staff and students as a means of reducing the risk of an attack being successful within the College.

The ICT department are also looking into the costs of Next Generation Antivirus solutions. This will offer better protection against malicious software than our current solution as it is more intelligent. It can also help with protecting against data loss.

The ICT department are currently reviewing the network infrastructure and planning upgrades to the WiFi and switches that will enable us to better control access to the college network.

The ICT manager is reviewing the current procedures for deploying updates to desktops and servers to ensure that the latest threats are mitigated as soon as possible. The ICT Manager and Infrastructure Technician are also looking into firmware updates for other network equipment to ensure that vulnerabilities are patched.

3. Recommendations

Members are asked to note the report and continue to monitor Cyber Security activities.

Billy Currie
Head of Corporate Services
February 2019

Audit Committee

WHISTLEBLOWING POLICY UPDATE

1 Purpose of the Report

The purpose of the report is to provide an update to members of the committee on the changes to the College's Whistleblowing Policy.

2 Background

The College, through normal processes is required to update policies and procedures on an ongoing basis. The Whistleblowing Policy was due for update. This previously sat with the Vice Principal (Corporate Services and Governance), however, given that it is a mechanism for staff to report suspected malpractice and other issues, it would better sit in the remit of Head of Human Resources. On review the Policy was found to be relevant and fit for purpose, however there are a few changes required to ensure it is up to date. These are detailed in Section 3.

3. Key Changes

The following changes have been made to the policy to ensure it is in line with best practice:

- Change in the title to include Public Interest Disclosure to reflect the change in terminology more widely used currently.
- Change of responsibility to Head of Human Resources to reflect the new structure and remits of posts in the College.
- Additional undertaking of the College to protect all parties involved in the process.
- Additional links to the disciplinary procedure for false or malicious allegations.

4. Conclusion

The Committee is asked to note the changes in the policy.

Carol Turnbull
Principal and CEO

PUBLIC INTEREST DISCLOSURE (WHISTLEBLOWING) POLICY

Strategic Aim	**To continue to maintain and improve the college's financial health and security**	
Responsibility	**Head of Human Resources**	**Michael Youd**
Issue Date	**16/01/2019**	
Revision Date	**15/01/2022**	
Equality Impact Assessment	**22/01/2019**	

Public Interest Disclosure (Whistleblowing) Policy

1 The Policy

Dumfries and Galloway College is committed to providing the means by which an individual may raise concerns which he/she may have about malpractice or corruption in the workplace. Members of staff are assured that genuine concerns which are raised will be investigated.

This policy outlines the means by which staff, consultants, contractors, volunteers, casual workers and agency workers may raise concerns without fear of reprisal or victimisation.

Students who may wish to raise concerns should do so following the College's complaints procedure.

All matters raised under this Policy will be treated in the strictest of confidence.

2. Definition of Malpractice or Corruption

This policy is not intended to provide a means for staff to express any dissatisfaction with their personal circumstances. Such matters should be raised through the College's Grievance Procedure.

This policy is intended to provide a way by which potential malpractice, corruption or extremism related activities may be reported in confidence, and without fear of reprisal.

The College regards malpractice, corruption and extremist activities to include (but not limited to):

a) criminal activity;
b) failure to comply with any legal obligation or regulatory requirement;
c) miscarriages of justice;
d) danger to health and safety;
e) damage to the environment;
f) bribery;
g) financial fraud or mismanagement;
h) negligence;
i) unauthorised disclosure of confidential information;
vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberties and mutual respect and tolerance of different faiths and beliefs
j) the deliberate concealment of any of the above matters.

3 The Process

3.1 Concerns should be raised in the first instance with the Head of Human Resources , or a member of the Executive Team if the concern is about the Head of Human Resources.

3.2 The Principal will be advised or if the concern is about the Principal, the Chair of the Board of Management, that an investigation is taking place.

3.3 An internal investigation will take place by the Head of Human Resources or nominated officer. However, depending on the nature of the complaint internal or external auditors may be the appropriate body to conduct an investigation.

3.4 If there is evidence of criminal or extremist activity then College Policy is that the police will be informed.

3.5 The complainant will be kept up to date with progress by the Head of Human Resources.

3.6 An employee who is not satisfied that their concern is being properly dealt with by the Head of Human Resources has the right to raise it with the Principal.

3.7 The complainant will be informed of any conclusions within 5 days of determination

4 Confidentiality

4.1 Any staff who raises a concern will have the right to have the matter treated confidentially. However, it should be noted that in some circumstances it will not be possible to pursue an accusation without revealing the name of the complainant to the individual being investigated. The College will protect all parties involved should this be necessary.

4.2 The confidentiality of the person[s] under investigation will also be respected and any investigation will be conducted with appropriate discretion.

5 False Accusation

5.1 Abuse of this policy by staff making false or malicious allegations or with a view to personal gain will be regarded as a serious offence and may be subject to disciplinary action. Should this be the case, a separate investigation into the matter may be required under the disciplinary procedure taking into account the findings of the investigation under this procedure.

5.2 It is a disciplinary offence to victimise or discriminate a member of staff who has raised a genuine concern under this policy.

6 External Disclosures

The process provides an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases individuals should not find it necessary to alert anyone externally.

However, the it is recognised that in some circumstances it may be appropriate for staff to report their concerns to an external body. The College strongly encourages staff to seek advice before reporting a concern to anyone external. The independent whistleblowing charity, Public Concern at Work, operates a confidential helpline. If staff wish to speak to someone outside the College, regarding whistleblowing, the charity can be contacted on 020 7404 6609 or by email www.pcaw.co.uk

7 Review

This policy will be reviewed every 3 years or in line with legislative or procedural changes.

DISTRIBUTION LIST

All Staff
Quality Manual

Audit Committee

ANTI FRAUD & CORRUPTION POLICY

1. Purpose of the Report

1.1 The purpose of this report is to provide an overview of the changes to the Anti-Fraud & Corruption Policy.

1.2 A copy of the revised Policy is included in the Appendix to this report.

2. Revisions to the Policy

2.1 The Anti-Fraud and Corruption Policy sets out the College's position in the prevention of fraud and response to fraud and corruption, including Key Principles and Responsibilities off the Board of Management, Executive Management Team and all staff.

2.2 Some minor changes have been made to the Policy to refer to the Code of Good Governance for Scotland's Colleges, and to the 2018 revisions to the UK Corporate Governance Code.

2.3 There is some overlap between this Policy and the Code of Conduct Policy and the College's Financial Regulations, and this Policy may require to be updated following the updates which are currently in progress for the Financial Regulations.

3. Recommendation

Members are asked to review the changes to the Policy and recommend it for approval by the Board of Management.

ANTI-FRAUD & CORRUPTION POLICY

Strategic Aim	**To continue to develop and ensure effective leadership, governance and management throughout the organisation**	
Responsibility	**Head of Finance**	**Karen Hunter**
Issue Date	**16/01/2019**	
Revision Date	**15/01/2022**	
Equality Impact Assessment	**22/01/2019**	

ANTI-FRAUD AND CORRUPTION POLICY

1.0 Introduction

1.1 One of the essential functions of public sector organisations is to ensure the proper use of public funds. This policy sets out the College's position in the prevention of and response to fraud and corruption.

1.2 In developing this policy, the College has taken account of existing external guidance and legislation, including the **Code of Good Governance for Scotland's Colleges**, the **UK Corporate Governance Code 2018** and **Bribery Act 2010**.

1.3 The College will treat any instances of fraud or corruption by its employees, board members, or contractors as serious breaches of discipline and as potentially criminal acts. Bribery of or by any College employee, board member or contractor for either personal or organisational gain will be similarly treated.

The College will co-operate fully with any criminal investigations carried out in response to instances of fraud, corruption or bribery.

2.0 Scope

2.1 The policy applies to all activities undertaken on behalf of the College by members of staff, members of the Board of Management and its subsidiaries.

3.0 Key Principles

3.1 The results of fraud and/or corruption can be costly, time- consuming, disruptive and unpleasant. The College, therefore, sees that the overriding principle to be applied is that of prevention. Where this fails, however, then reporting, investigation and, where necessary, sanctions, will be pursued rigorously and swiftly.

3.2 The College adheres to the Bribery Act 2010 which covers, amongst other things, the offences of bribing another person, of allowing to be bribed and organisational responsibility. Such offences include:

- The offer, promise, or giving of financial or other advantage to another person in return for the person improperly performing a relevant function or activity.

- Requesting, agreeing to receive or accepting a financial or other advantage intending that, in consequence a relevant function or activity should be performed improperly.

3.3 Preventative measures are identified under five broad headings: -

3.3.1 *Policies and Procedures*

The College shall develop, implement and maintain such policies and procedures

so as to reduce, as far as possible, the risks from fraud or corruption. These will include: -

- Risk Management
- Financial Regulations
- Procurement
- Scottish Public Finance Manual
- Scheme of Delegation
- Financial Memorandum

3.3.2 *Systems*

The College will maintain in place systems which incorporate internal controls, including adequate segregation of duties to ensure that, as far as possible, fraud and corruption can be prevented.

3.3.3 *Internal Audit*

The College will ensure that it agrees a programme of internal audit assignments to support the systems and procedures already in place and to assist in the reduction of the likelihood of fraud.

3.3.4 *Culture*

The College will maintain a culture of openness, honesty and accountability. This will be supported by the following policies and procedures:

- Code of Conduct Policy
- Public Interest Disclosure (Whistleblowing) Policy
- Disciplinary Procedure (Staff)

3.3.5 *Staff Recruitment, Induction and Training*

The College will ensure references are taken up for all permanent and temporary staff. As part of induction, staff will be made aware of all policies and procedures pertinent to their post, including those concerning governance.

3.4 The principles to be observed for the reporting and investigation of fraud and corruption are as follows: -

3.4.1 Concerns should be reported in accordance with the College's Public Interest Disclosure (Whistleblowing) Policy. A detailed investigation of any concerns will be undertaken.

3.4.2 The College will deal with any instances of fraud or corruption swiftly, taking disciplinary action as necessary and informing the police if appropriate in accordance with the Disciplinary Procedure (Staff).

3.4.3 In the event that fraud is suspected on the part of contractors, agency workers or by staff involved in agency or contract work on behalf of other bodies, procedures and

responsibilities for reporting and investigation are the same as for staff. The College will also inform and involve employing contractors or agencies when appropriate.

4.0 Responsibilities

4.1 The Board of Management is responsible for ensuring the effectiveness of internal control of the College, based on information provided by the Executive Management Team.

4.2 The Audit Committee is responsible for agreeing this policy and monitoring its implementation and effectiveness.

4.3 The Executive Management Team is responsible for developing appropriate systems of internal control to reduce the likelihood and impact of fraud or corruption.

4.4 The Head of Finance is responsible for the implementation of this Policy.

4.5 Operational managers are responsible for the application of internal controls to mitigate risks within their specified areas of responsibility.

4.6 All staff members are responsible for adhering to the systems of internal control which are relevant to their role.

5.0 Review

5.1 This policy will be reviewed every 3 years or whenever Corporate Governance changes affect any part of it.

DISTRIBUTION LIST

All Staff
Quality Manual

Audit Committee

Risk Management Policy

1 Purpose of the Report

During the summer 2018 the Principal undertook to review the presentation and format of the strategic risk register in terms of appropriateness of risks, and risk measurement and controls. The new format was approved by the Audit Committee and, subsequently the full Board of Management early in academic session 2018-19.

The attached paper is an updated Risk Management Policy which reflects these changes.

2 The Report

The Risk Management Policy has been rewritten in its entirety to reflect the purpose, scope, and identification and management of risk and to reflect changes in the format of the Strategic Risk Register and College Management Structure that impact on the policy.

A copy of the original Risk Management Policy is also attached for reference.

3 Recommendation

The Audit Committee is asked to review and approve the updated Risk Management Policy.

Carol Turnbull
Principal
February 2019

Audit Committee

RISK MANAGEMENT POLICY

Responsibility	**Vice Principal Corporate Services & Governance**
Issue Date	**13/06/2016**
Review Date	**12/06/2019**

Audit Committee

1 Purpose of the policy

The purpose of the risk management policy is to outline the college approach to risk management and define the key principles, processes and responsibilities for the management of risk across the organisation. This policy forms part of the College's internal control and corporate governance arrangements.

2 Objective of risk management

The objective of undertaking risk management is to provide a systematic way of identifying, recording, monitoring and reporting risks to ensure the organisation is able to meet its objectives.

3 Principal documents

The identification and management of risk affecting the organisation's ability to achieve its objectives are set out in college strategic plan and in other planning documents such as college regional outcome agreement. These contain the key responsibilities of all members of staff and partners involved in the college's work.

The effective management of risk is an important means by which the organisation achieves its goals. To that end the college policy is designed to:

- manage risk actively across the full range of activities
- devolve responsibility for risk ownership and management to the most appropriate level whilst maintaining clear overall executive management responsibilities
- integrate risk management with planning at department and corporate levels
- encourage a risk aware way of working
- accept levels of risk that are compatible with professional responsibilities and take account of stakeholder expectations
- monitor and report regularly on the management of risk

4 Nature and context of risk

Risk can be defined as the threat that an event, action or inaction will adversely affect the organisation's ability to achieve its objectives.

Risks can be strategic or operational in nature. It is possible to control some risks and to influence others but there will be some that are outside management control or influence. Risk management takes these factors into account in judging the acceptable level of risk and the actions needed to reduce the risk level.

5 Implementing the risk management policy

5.1 Roles and responsibilities

Risk management is an integral part of the overall governance arrangements of the College. As such there are specific responsibilities for people and groups undertaking different roles in the organisation:

5.2 Board of Management

The Board of Management has ultimate responsibility for the management of risk within the College. This includes:

- determining the appropriate risk appetite for the College;
- or level of setting the tone at the top for risk management throughout the organisation;
- approving the overall risk management arrangements including this policy and the appetite for risk;
- consideration of reports on the operation of risk management arrangements through the Audit Committee, the Principal and annual assurances for completion of annual report and accounts.

5.3 Audit Committee

Detailed consideration of the operation of risk management arrangements is delegated to the Audit Committee. This role includes:

- consideration, at each meeting of the corporate level risk register;
- consideration of internal audit reports involving risk or risk management;
- consideration of external audit reports involving risk or risk management;
- advising the Board on annual assurances involving risk and risk management included in the annual report and accounts.

5.4 Accountable Officer

The Principal has specific personal responsibility for signing the annual accounts including the Statement on the System of Internal Control**.**

5.5 Executive Management Team

The Executive Management Team has day to day responsibility for the management of the system of internal control including risk management. This role includes:

- encouraging a culture of risk awareness and risk management
- consideration of risk related procedures, strategies and registers
- ensuring that risks and risk management are included in project proposals or work plans presented to it for consideration or approval
- ensuring that there is ownership for all significant risks by a named member of the Senior Management Team

5.6 Staff, partner organisations and contractors

Members of staff and partner organisations or contractors are expected to:

- be familiar with the policy on and approach to risk management
- to be risk aware in their work
- to take responsibility for the ownership of risks assigned to them
- to inform managers if they become aware that business objectives could be at risk
- to take a corporate approach to risk by considering the implications for the whole organisation of individual risk management actions

This risk management policy and the risk register will form part of induction training for new staff.

Audit Committee

5.7 Risk register

The college will maintain a corporate level risk register under the ownership of the member of executive management responsible for planning. The register will be updated and considered regularly by the Executive Management Team and considered by the Audit Committee at each scheduled meeting. The Audit Committee is responsible to the Board of Management for monitoring, updating and raising awareness of risk levels. The main annual update is carried out in parallel with corporate planning processes.

The corporate risk register is intended to cover corporate wide risks and risks to corporate developments. Risks to individual projects are recorded and reported through operational planning and Executive Management Team monitoring processes unless they are so significant or pervasive that they pose a risk to corporate level objectives, at which point they are added to the corporate risk register.

Individual projects with a value over £50k or require constant active monitoring will carry a separate risk register throughout the life of the project.

5.8 Structure of the risk register

The register will include the following components for each risk:

- inherent risk assessments of likelihood and impact
- controls/actions in place to mitigate the inherent risks
- residual risk assessments of likelihood and impact
- further actions or monitoring required including timescales and reference to any relevant Key performance Indicators
- identity of risk owner

5.9 Risk scoring and risk appetite

The likelihood and impact of each risk is scored in accordance with Table A below. A definition of the categories of impact is provided in Table B below.

Traffic lights are used to identify the highest scoring Residual risk assessments which will be those requiring the greatest Board of Management / Senior Management Team attention. For Residual risk assessments Table C indicates the organisation's appetite for different levels of risk.

Any risks which have impacts on strategic objectives must have mitigating controls in place. Any risks with an inherent rating of 12 or above must have mitigating controls in place and where the residual rating remains above 12 should be reviewed at least quarterly in order to identify if any further actions could be taken to reduce the residual rating to below 12.

Table A:

		LIKELIHOOD			
IMPACT	**Multiplier**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Multiplier		**1**	**2**	**3**	**4**
Major	**4**	4	8	12	16
Moderate	**3**	3	6	9	12
Minor	**2**	2	4	6	8
Insignificant	**1**	1	2	3	4

Audit Committee

Table B:

IMPACT	Financial	Health and Safety	Reputation	Strategic Aims
Major	Reduction in SFC grant >£250k	Loss of life, permanent disability	National press	Not able to deliver on an aim
Moderate	Reduction in SFC grant between grant £100-250k	Serious injury (not permanent)	Significant local press (region wide)	Increased cost to deliver an aim
Minor	Reduction in SFC grant between £50-100k	RIDDOR Report (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995).	Minor local press	Delay on delivering an aim
Insignificant	Reduction in SFC grant <£50k	No perm injury	No press	No impact

Table C:

Residual risk assessment	Risk appetite response
12-16	Unacceptable level of risk exposure which requires immediate corrective action to be taken
6-9	Acceptable level of risk that requires constant monitoring and action to be taken to reduce exposure
1-4	Acceptable level of risk exposure subject to regular active monitoring measures

5.10 Other risk management arrangements

Risk management is also included in the project planning for major corporate projects. The nature and extent of documentation will depend on the significance of the project and the risks involved. Where major projects are concerned the risk may also appear at the corporate level – this does not obviate the need for specific risk management and ownership at the project level.

6.0 Review

6.1 This policy will be reviewed every 3 years or whenever Corporate Governance changes affect any part of it.

DISTRIBUTION LIST

All Staff Members
Quality Manual

RISK MANAGEMENT POLICY

Responsibility	**Vice Principal Business Development & Corporate Services**
Issue Date	
Review Date	

Contents

1. Purpose

The purpose of this policy and related arrangements is to:

- Outline approaches and arrangements in respect of the management, oversight, control, mitigation, evaluation and reporting of risks associated with College operations and activities;
- Ensure that significant risks are monitored and managed more closely; and
- Confirm the roles and responsibilities of the Board of Management, Executive Management Team and others in the effective management or risks.

2. Scope

This policy covers the management of financial, strategic, operational, reputational and project-based risks related to all aspects of College activities and operations, including those where the College is operating in partnership with others.

This policy is approved by the Audit Committee of the Board of Management and will be subject to regular review by the Committee in line with College document control and review procedures.

It should be noted that this policy does not cover arrangements in respect of health and safety risk assessment, which is managed under the terms of the College Health & Safety Policy.

3. Identification and Management of Risk

The development of effective risk management arrangements are essential to control and manage the risks that may otherwise threaten the ability of the College to meet its objectives.

Risk management is bound inextricably within the system of internal control that operates across the College. This system encompasses a number of elements that together ensure that effective and efficient outcomes are achieved, allowing the College to respond to strategic and operational risks. These elements include the following:

3.1 Strategic Risk Framework

High-level strategic risks are outlined with a clear risk register that links directly to the College Regional Outcome Agreement (ROA). These risks are discussed and approved by the full Board of Management. This framework is integrated with strategic planning arrangements and relates directly to strategic developments and detailed analysis of the regional operating context for the College.

Within these arrangements, the Executive Management Team undertake the ongoing monitoring mitigation of risks significant to the College. The strategic risk register is formally reviewed and updated quarterly through the Board of Management Audit Committee.

Risks are managed based on a series of risk factors determined by assessment of the likelihood multiplied by the impact of each specific risk using a scale of 1 (low) to 5 (high).

Each risk factor is colour coded as follows:

Green	Low risk factor (Minor risk)	1 – 8
Amber	Medium risk factor (Significant risk)	9 – 14
Red	High risk factor (Fundamental risk)	15 and above

Each risk is assessed and categorised prior to the actions taken to manage the risk and again following assessment of the mitigating actions in place. Where a post mitigation risk is highlighted as red this will be subject to review at each subsequent meeting of the Board of Management Audit Committee.

3.2 Regional Outcome Agreement (ROA) Activity Planning

The detailed activity planning arrangements linked to the ROA are used to set outcome targets and objectives, inform budget plans and identify risks associated with College activities. Progress towards meeting ROA activity plans is reviewed through the use of the ROA measurement plan and is monitored on a rolling basis throughout the year and reported through the annual ROA self-evaluation report.

3.3 Quality Management System

The College operates a documented quality management system. This system provides a clear structure of policies, procedures, quality processes and other documentation that underpin the control and review of key College processes and their related risks.

All sections of the quality management system are approved at Executive Management Team level, with reference to the Board of Management where appropriate.

3.4 Operational Risk Frameworks

Managers ensure that significant risks related to the outcomes, activities and operational objectives of their area of responsibility are identified, assessed and monitored. Operational risks are appraised on a rolling basis through team/project meetings and emerging risks are communicated and managed as required. Where necessary, the impact of risks in respect of the achievement of operational outcomes is detailed within self-evaluation records.

3.5 Determination and Management of Project-based Risks

Approval of all capital and revenue projects where College contribution is in excess of £250k in value will include the requirement to create and manage specific risk register in relation to the project or activity. This determination and rating of risk must include the following:

- Risks impacting on project/College objectives
- Significant financial and other operational risks
- Reputational or other risks

Project based risk registers may be necessary in other circumstances where the nature of the project or the level of non-financial risk involved warrants this.

3.6 Internal Audit Arrangements

The Board of Management Audit Committee determines and approves a rolling annual schedule of internal audit activities designed to check and test internal control and risk management arrangements. Analysis and feedback in respect of risk and control issues is used to inform development and prioritisation of this schedule. The schedule includes the internal audit review of risk management approaches, arrangements and effectiveness.

3.7 External Audit Arrangements

External audit provides feedback to the Audit Committee on the operation of the internal controls reviewed as part of the annual audit requirements specified by the Scottish Government and Scottish Funding Council.

3.8 Quality and Third Party Monitoring

Internal and external reviews and reports in respect of the achievement of required outcomes and compliance with systems are used to inform potential risks and to strengthen internal control systems as appropriate.

3.9 Management Reporting Arrangements

Regular reporting through a range of management channels including: Executive and College Leadership Team meetings, team meetings and project and system planning groups is designed to monitor key risks and their controls.

Decisions to rectify problems are made through these regular reporting activities and priorities, impacts or concerns are reported to the College Leadership Team and/or the Board as necessary.

To underpin these arrangements extensive use if made of clear and comprehensive data through real time reporting from College systems and the development and review of a broad range of business intelligence reports.

3.10 Annual Report Arrangements

The Board of Management is responsible for reviewing annually the effectiveness of risk management arrangements and outcomes, based on information provided by the independent auditors (internal and external) and the Executive Management Team.

To inform this the Audit Committee will consider annually a report produced by the internal auditors that summarises the outcomes of audit activities and provides a clear opinion in respect of the robustness of the internal controls in place and any other significant factors found.

Detailed evaluation reports in respect of the achievement of the College ROA and on the quality of learning, teaching and services will be discussed and approved annually by the full Board. These will be considered alongside financial performance and other metrics as considered appropriate.

3.11 Business Continuity Planning and Disaster Recovery

The College maintains a business continuity plan providing a framework within which serious incidents or other significant events that may impact on business continuity are managed.

Disaster recovery arrangements are in place in respect of all major ICT systems operated by the College.

4. Responsibilities

4.1 Role of the Board of Management

The Board of Management has responsibility to provide leadership within a framework of effective controls, which enable risk to be assessed and managed. The Board of Management has responsibility through the operation of the Board and each Board Committee to monitor, challenge and oversee risk management within the College as a whole.

Within all of these arrangements, it is the responsibility of the Board of Management to:

- Establish the overall culture and ethos in respect of risk and opportunity management within the College
- Determine the appropriate risk appetite (the level of exposure with which the Board is comfortable) for the College that balances risk with opportunity

- Approve major decisions affecting the College risk profile or exposure in accordance with appropriate financial strategy and procedures and agreed delegation limits

- Ensure that risk management is integrated in strategic planning activities and outcome agreements

- Monitor the management of key risks (those rated in excess of the risk appetite) to reduce their probability and impact

- Satisfy itself that the less significant risks are managed, and that risk controls are in place and working effectively

- Annually review the College approach to risk management and approve changes or improvements as necessary

4.2 Role of the Audit Committee

The Board of Management has delegated responsibility for risk management to the Audit Committee.

The Audit Committee will monitor and report to the Board on internal controls and alert Board members to any significant emerging issues. In addition, the Committee oversees internal audit, external audit and management as required in its review of internal controls.

The Audit Committee will report to the Board annually on the effectiveness of the internal control system, including the College system for the management or risk.

4.3 Role of the Executive Management Team

As the senior management group of the College, the Executive Management Team have overall operational responsibility for the identification, management and mitigation of risk in line with Board objectives and risk appetite.

It is the role of the Executive Management Team to provide advice and guidance to the Board in respect of potential and actual risk issues and to implement appropriate risk management and internal controls on an ongoing basis. The Executive Leadership Team will also be asked to provide accurate, timely and clear information to the Board of Management and its Committees to support Board members in understanding and evaluating the status of risks and controls.

Within these responsibilities, the Vice Principal Business Development and Corporate Services will review annually the effectiveness of the system on internal control and provide a report on this to the Board of Management through the Audit Committee.

4.4 Role of Managers

All staff with a management of team leadership role are responsible for ensuring that good risk management practices are developed and adopted within their area of responsibility. This will include the creation, implementation and review of operational risk registers for their area of service.

5. Implementation

To support implementation of this policy all staff with responsibilities under the terms of the policy will receive appropriate guidance, support and training in relation to these responsibilities.

6. References

- Board of Management Articles and Committee Remits
- Code of Good Governance for Scotland's Colleges
- Strategic and operational risk registers
- Regional Outcome Agreement
- Head of Planning & Quality
- Finance Procedures
- Internal audit schedule and reporting
- Business Continuity Plan

7. Review Details

Next Review Scheduled for: XX.XX.XX

Responsibility for Review: Audit Committee and Vice Principal

Union Consultation Required: No

OUTSTANDING AUDIT RECOMMENDATIONS Updated - 08.02.19

- Review of Medium and High Risk Recommendations to be followed-up

		Number:
KEY:	**Complete, to be included in Follow-up review**	14
	In progress	4
	Added to report from recent audit review	0
		18

Ref	Original Recommendation	Internal Audit Report/ Date	Original Comments	Proposed Implementation Date	Owner responsible	Update
1	The Facilities Manager will investigate how to record quality control checks that have been completed on contractors' and janitors' works.	Follow-Up 04.18	A quality control question will be added to the TSR form for originators of jobs to answer, to ensure that quality checks on janitors' jobs are being checked.	September '18	Facilities Manager	Satisfaction' question now sent on completion of TSR, and further actions are dealt with by the relevant manager.
2	The TSR system is capable of producing performance indicators; however, currently the performance indicators the system produces only show how many requests have been received and how many have been completed in a month. The performance indicators on the system are not used by the Estates team to monitor performance of completing reactive maintenance requests.	Follow-Up 04.18	We will discuss which key performance indicators the Estates team should have in place and what the target level is for each of these indicators. The Maintenance Foreman will review and discuss KPIs with janitorial staff on a monthly basis, to identify the reasons why any KPIs have not been achieved and any areas they need to improve on as a team, and also to highlight what they are doing well. An update on reactive maintenance KPIs will be provided to the Finance and General Purposes Committee as part of the general performance update on estates and facilities.	September '18	Facilities Manager	KPI's now in place, to run alongside of SLA
3	By not having a system in place which can automatically generate daily, weekly and monthly sales reports there is a risk that all the sales may not be captured.	Follow-Up 04.18	From session 2017-18 each curriculum area will have income generation targets monitored through PMR system.	May '18	Finance Manager	Consideration of 'commercial sales' targets for each curriculum discussed with CM's/ original recommendation now superseded due to joint Curriculum Planning with Academic areas and CTS, and consideration of developments being implemented - individual targets are not considered to be appropriate, however an overall income target will be set for the College.

OUTSTANDING AUDIT RECOMMENDATIONS Updated - 08.02.19

- Review of Medium and High Risk Recommendations to be followed-up

		Number:
KEY:	**Complete, to be included in Follow-up review**	14
	In progress	4
	Added to report from recent audit review	0
		18

Ref	Original Recommendation	Internal Audit Report/ Date	Original Comments	Proposed Implementation Date	Owner responsible	Update
4	ICT management will ensure that software updates are applied consistently to IT assets such as servers and desktops in accordance with the patch procedure.	Follow-Up 04.18	ICT management will consistently apply the Windows 10 program update to all of the College's desktops.	August '18	IT Manager	A number of computers have now been updated to Windows 10. The next phase is currently being rolled out, and the new ICT Manager aims to have this completed in 3 months
5	The costing model should be reviewed to ensure staffing costs are consistently applied	Complete Training Solutions 03.18	All costs will be reviewed for the programme for Academic Year 2018-19 including Modern Apprenticeship academic delivery and staff on costs	June '18	Business Development Manager and Finance Manager	The costings model has been revised, and a report prepared for COT to review the main assumptions
6	Feedback from external events to inform courses is not formally documented, and without an employment engagement strategy, the College may fail to engage with appropriate employers and be able to provide courses to them, resulting in a missed opportunity for income.	Complete Training Solutions 03.18	A documented employer engagement strategy will be developed	June '18	Vice Principal Learning and Skills	Employer Engagement Strategy is now in place
7	The contribution targets include programme delivery costs but not all student costs.	Complete Training Solutions 03.18	All contribution targets will be reviewed and agreed when the costings working document is updated for Academic Year 2018-19.	June '18	Executive Management Team	The costings model has been revised, and will be fully implemented in 2019-20
8	There is no central point for induction checklists to be uploaded to, these are retained by the individual tutors on individual student files. Without a central point for the storage of induction checklists, there is a risk that the College is unable to evidence that inductions have taken place.	Student Journey 04.18	All induction checklists will be uploaded to the Adminnet system.	October '18	Heads of Curriculum	All Induction Checklists are now being held centrally with the Quality team
9	Without documented reasons for withdrawal, there is a risk that the College may not follow up with students resulting in a lost opportunity to improve provision and subsequent students may withdraw	Student Journey 04.18	Where students withdraw, their tutor will detail on Adminnet or on the SR9 withdrawal form what action they had taken to get in touch with the student and why they have been withdrawn from the course.	August '18	Heads of Curriculum	All Curriculum managers have now been directed to include details on SR9 forms
10	Procedures for dealing with student withdrawals - the required date for attendance had been input incorrectly on the SITS system.	Student Activity Data 09.18	The College will ensure that the required attendance date is correctly calculated on the SITS calculator	November '18	Business Systems Manager / Student Records Manager	All now fully implemented/ dates all now checked

OUTSTANDING AUDIT RECOMMENDATIONS Updated - 08.02.19

- Review of Medium and High Risk Recommendations to be followed-up

		Number:
KEY:	**Complete, to be included in Follow-up review**	14
	In progress	4
	Added to report from recent audit review	0
		18

Ref	Original Recommendation	Internal Audit Report/ Date	Original Comments	Proposed Implementation Date	Owner responsible	Update
11	The required date for part-time students had been calculated based on the student being full-time - without accurate required attendance dates, there is a risk that students could be included in the credit return without attending 25% of their part-time course.	Student Activity Data 09.18	The College will ensure that the required attendance date is correctly calculated on the SITS calculator for all part-time courses. The Student Records Manager will conduct a manual calculation of part-time courses required attendance dates to ensure they are accurate. This check will be conducted quarterly	November '18	Business Systems Manager / Student Records Manager	All now fully implemented/ dates all now checked
12	For staff working in specific areas e.g. engineering and construction, specific health and safety training may be required to use certain machinery.	Health & Safety 11.18	Heads of Department will be requested to produce lists of equipment and machinery within their department which requires additional safety training as well as identifying the staff who operate this machinery within their role. Also Health and safety audits will now include a review of these equipment lists and a review of training records against these lists to ensure staff operating machinery are appropriately trained.	March '19	Head of Corporate Services	A new internal checklist has been revised to include the recommendations from the audit. This has been issued to all managers for awareness before any checks are carried out.
13	Roles and responsibilities for RIDDOR reporting are clearly defined.	Health & Safety 11.18	The Health and Safety Policy is due to be updated shortly by the newly formed Health and Safety Committee, RIDDOR requirements and guidance will be included as part of this review.	February '19	Head of Corporate Services	The policy has been revised with the inclusion of the wording for RIDDOR.
14	Health and safety is monitored at the Health and Safety Committee where information regarding statistics, trends and other relevant health and safety issues are discussed	Health & Safety 11.18	A new Health and Safety Committee is being recruited and will meet on a quarterly basis. Its first meeting will develop a Terms of Reference and present to the Board for approval.	January '19	Head of Corporate Services	New members have come forward for the committee. First meeting due in February.
15	Health and safety statistics, as well as details of compliance against legislation, are not reported at board level on a frequent basis.	Health & Safety 11.18	Health and safety will become a standing item on the monthly senior management team meeting where the Health and Safety Manager will present an update on key details relating to health and safety.	January '19	Head of Corporate Services	Now fully implemented/ included as a standing item on the CLT Agenda

OUTSTANDING AUDIT RECOMMENDATIONS Updated - 08.02.19

- Review of Medium and High Risk Recommendations to be followed-up

		Number:
KEY:	**Complete, to be included in Follow-up review**	14
	In progress	4
	Added to report from recent audit review	0
		18

Ref	Original Recommendation	Internal Audit Report/ Date	Original Comments	Proposed Implementation Date	Owner responsible	Update
16	We recommend that the College investigates the finance system capabilities and whether electronic journal authorisation of journals is possible. In whatever system is used, the College should ensure there is clear evidence of approval for all manual journals.	External Audit 11.18	We will liaise with our software provider to investigate if an approval procedure could be set up within the finance system. If that isn't possible we will include a manual check for authorisation of all journals as part of the monthly process.	November '18	Head of Finance	Civica have advised that this isn't possible using the finance software. A process has been set up using the Nominal ledger daybook and this will be carried out as part of the monthly accounts completion
17	The billing arrangements with UWS for staffing re-charges should be agreed in sufficient detail that the College is able to estimate the amount of income it will receive	External Audit 11.18	We will liaise with the University of the West of Scotland to establish a formal agreement for the teaching contract	December '18	Head of Finance	HoF is liaising with UWS to set up a Service Level Agreement
18	The College should complete the review of the Financial regulations and authorised signatory listing and ensure these are appropriately authorised by the Finance and General Purposes Committee.	External Audit 11.18	We will complete the update of the Financial Regulations and authorised signatories as per of the 2019-20 budget planning process.	March '19	Head of Finance	Revised Financial Regulations are being drafted

DUMFRIES AND GALLOWAY COLLEGE

Internal Audit Progress Report

19 February 2019

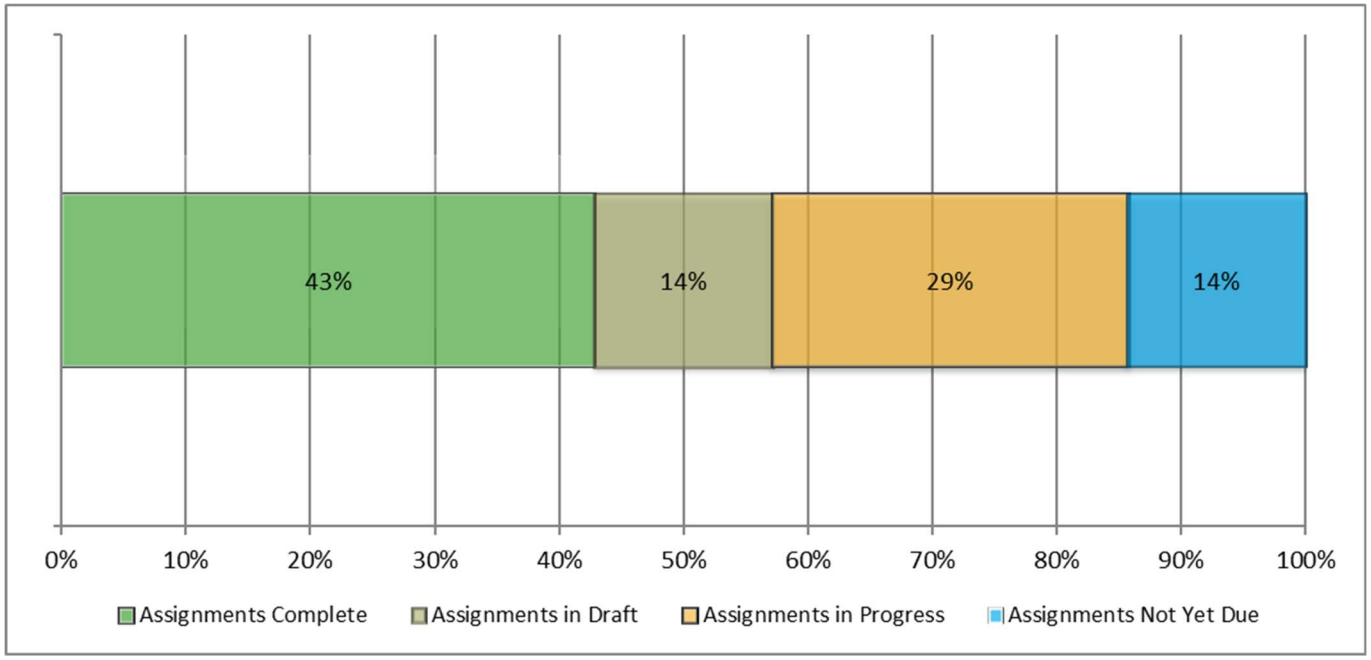
RSM

CONTENTS

1 INTRODUCTION

The internal audit plan for 2018 / 2019 was approved by the Audit Committee on 17 May 2018.

The table below provides a summary update on progress against the 2018 / 2019 plan.



2 LOOKING AHEAD

Assignment area	Proposed audit timetable	Target Audit Committee
Key Financial Controls: Creditors	Draft report issued	May 2019
Equality and Diversity	Fieldwork completed	May 2019
Follow Up of Previous Internal Audit Management Actions	Fieldwork completed	May 2019
Financial Planning / Forecasting	Week commencing 8 April 2019	May 2019

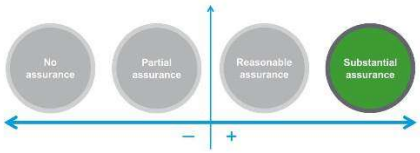
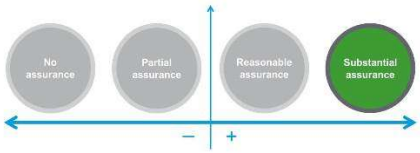
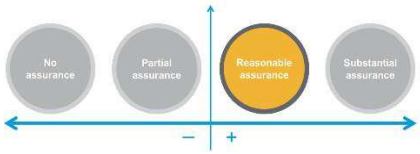
3 OTHER MATTERS

3.1 Key performance indicators (KPIs)

Delivery			Quality		
	Target	**Actual**		**Target**	**Actual**
Draft reports issued within 10 working days of debrief meeting	10 working days	*4 working days (average)*	Conformance with PSIAS and IIA Standards	Yes	*Yes*
			Liaison with external audit to allow, where appropriate and required, the external auditor to place reliance on the work of internal audit	Yes	*As and when required*
Final report issued within 3 working days of management response	3 working days	*1 working day (average)*	% of staff with CCAB/CMIIA qualifications	>50%	*67% ytd*
			Turnover rate of staff	<10%	*No staff turnover in 2018 / 2019*
			Response time for all general enquiries for assistance	2 working days	*2 working days (average)*
High & Medium recommendations followed up	Yes	*Yes*	Response for emergencies and potential fraud	1 working day	*N/A*

APPENDIX A: INTERNAL AUDIT ASSIGNMENTS COMPLETED TO DATE

Reports previously seen by the Audit Committee and included for information purposes only:

Assignment	Opinion issued	Actions agreed		
		L	M	H
Student Support Funds		2	0	0
Student Activity Data		0	2	0
Health and Safety		2	2	0

FOR FURTHER INFORMATION CONTACT

Rob Barnett, Head of Internal Audit

RSM
St. James' Gate
Newcastle Upon Tyne
NE1 4AD

M: 07809 560103
Robert.Barnett@rsmuk.com

rsmuk.com

Dear Finance Manager,

Audit Scotland Statutory fees for Dumfries and Galloway College – 2018/19 audits

The purpose of this email is to give you an indication of the fees for 2018/19 audits. This is based on Audit Scotland's overall budget proposals that will be considered by the Scottish Commission for Public Audit (SCPA).

In a change to previous notifications the fee for your audit can be identified by clicking on the link Fee_Setting and following the detailed instructions worksheet. On selection of your organisation(s) the expected fee will be provided together with a comparison against the final agreed 2017/18 fee. The document can be found on our website - http://www.audit-scotland.gov.uk/about-us/audit-scotland/audit-appointments.

Fee setting arrangements
Audit fees are based on our funding & fee strategy which was revised in 2016 following consultation with stakeholders. The two key principles for our fee setting arrangements are:

- Audit fees should be set with the objective to recover the full cost of audit work in each sector

- The cost of the audit should be independent of the identity or location of the auditor.

The expected fee for each body assumes that it has sound governance arrangements in place and operating effectively throughout the year, prepares comprehensive and accurate unaudited accounts and meets the agreed timetable for audit.

The actual amount you will pay will depend on the amount of the audit fee agreed with your auditor. Fees can be agreed between the auditor and the audited body by varying the auditor remuneration by up to 10% above the level set (20% for bodies with an expected fee below £26,000), for example, where significant issues require additional work to be undertaken. In exceptional circumstances higher remuneration can be agreed with the prior agreement of Audit Scotland.

Invoices
Audited Bodies in the Central Government - chargeable, NHS, Local government and Scottish Water sectors will shortly be issued with invoices for a payment on account, based on 1/3 of the expected fee. Further instalments (adjusted for the amount of the fee agreed with the auditor) will be invoiced in March/April 2019 and August 2019.

The expected fee information for Central government - non chargeable bodies is notional and no invoices will be issued as they are funded by Parliament.

Further Education bodies invoices will be issued in September 2019 and May 2020.

If your Accounts department requires a purchase order number to be quoted on invoices for processing please could you arrange for this to be raised as soon as possible and send your order to the email address remit@audit-scotland.gov.uk. Please ensure that the order is based on the full expected fee to allow us to quote this on all instalment invoices.

A final invoice will be issued if necessary, once all 2018/19 audits are complete, to adjust for any late changes to agreed fees.

Please let me know if there is anything that you wish to clarify or discuss further.

Yours sincerely

Stuart Dennis
Corporate Finance Manager
Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
T: 0131 625 1626 E: sdennis@audit-scotland.gov.uk
www.audit-scotland.gov.uk

Expected audit fee

Instructions

AUDIT SCOTLAND

Year 2018/19

Sector Further education **Body** Dumfries and Galloway College

	Auditor	Auditor	Pooled	Contribution	Contribution to		Total:	Agreed Fee
2018/19	Scott-Moncrieff	14,060	810	-	850	**£**	**15,720**	**To be agreed**
2017/18	Scott-Moncrieff	13,740	880	-	760	£	15,380	£ 16,070
Difference (£)		320	-70		90		**340**	
Difference (%)		2.3%	-8.0%		11.8%		**2.2%**	

Summary

Overall fees within the Further education sector have increased by 2.2%

The expected fee for Dumfries and Galloway College for the 2018/19 audit is £350 lower than the fee agreed the previous year (2.2%).

Audit Committee

FEEDBACK REQUEST – EXTERNAL AUDIT

1. Purpose of the Report

1.1 The purpose of this report is to inform the Committee that Audit Scotland have advised that they are keen to hear from the College about the quality of audit work provided by our external auditors for last year, to inform their assessment of audit quality.

1.2 Audit Scotland have advised that they intend to issue an on-line questionnaire which will include tailored questions for Directors of Finance, Chairs of Audit Committees and Chief Executives.

1.3 A survey was issued by Audit Scotland which related to the 2013-14 audit and included a number of questions aimed at identifying scope for improvement in auditors' work and the impact of the audit.

1.4 Audit Scotland have not indicated a timeframe for the current survey.

2. Audit Scotland Message

2.1 The full text of the Audit Scotland message is as follows:

We are keen to hear from you about the quality of audit work provided by your external auditor for Dumfries and Galloway College in the last year. Your experience of the audit process is a critical part of our assessment of audit quality.

We have commissioned Mark Diffley Consultancy and Research (MDCR) to carry out this work on our behalf. This is a change from our previous in-house approach. MDCR bring greater independence and expertise to this process. This is the first year of a long term approach to increase our understanding of stakeholders' experience of external audit.

MDCR will be writing to a small number of bodies shortly to test a draft questionnaire to ensure that the questions are clear and capture high quality responses. MDCR will then be in touch with you to explain how the surveys will work. This will include tailored questions for Directors of Finance, Chairs of audit committees (or equivalent) and Chief Executives (or equivalent).

The survey will be online, brief, and should only take around 10 minutes of your time. We will review responses and where we identify themes we will discuss these with auditors and may carry out targeted work to better understand the nature of the concerns so that auditors can provide a better quality audit.

Audit Committee

Survey responses will be confidential and will be used only to assess the quality of audit work that auditors have provided. You will be given the option to opt out of the survey if you do not want to take part. If you have any concerns about the survey, please feel free to get in touch with me.

I look forward to your contribution to this process.

Regards,

John Gilchrist,
Audit Quality and Appointments Manager

Audit Committee

Strategic Risk Register

1 Introduction

1.1 The purpose of this paper is to provide the Committee with the opportunity to review the College's Strategic Risk Register.

2 The Report

2.1 The Principal and Executive Management Team routinely review the Strategic Risk Register to reflect the risks the College is facing and the mitigation that will be applied to each risk. There are currently 22 strategic risks, 5 of which are rated 9 (Amber = Significant risk) or above.

2.2 **Committee Reporting**

The Strategic Risk Register is now presented at each Committee and members are asked to pay particular attention to risks pertaining to the work of that Committee. The end column on the Risk Register has been amended to include the name of the Committee who would have 'oversight' of that risk, so that members can focus on these in their discussions. There is still the opportunity to discuss other risks at full Board meetings.

Changes have been made to the following:

- Risk No 2.6 - 'Failure to achieve credit targets'
  The likelihood has been reduced to 1. The College is currently only 400 credits short of its overall target and is confident that these will be achieved prior to the year end. The ring fenced Early Learning and Childcare credit target has been achieved.

- Risk No 2.7 – 'Insufficient Student Support Funding to meet Demand'
  Following confirmation from SFC that the College will receive the full additional funding allocation requested the likelihood of this risk has been reduced to 1.

- Risk No 3.5 – 'Industrial Relations Problems'
  No change to risk factors but updated to highlight that EIS are currently undertaking Industrial Action.

- Risk No 3.9 – 'Failure to reach aspirational standards in learning, teaching and service delivery'
  Latest PI reports indicate that there is no significant improvement in retention rates at either HE or FE level. The likelihood of this risk has been increased to 3 and the impact increased to 4. This risk is now Amber.

3 Recommendation

3.1 It is recommended that the Committee consider and, if so minded, approve the Strategic Risk Register.

Carol Turnbull
Principal
February 2019

Post Holders							
	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
1	**Strategic and Structural**									
1.1	Failure of College strategy to meet the needs of Dumfries and Galloway Region and/or national priorities (eg Employability, DYW, attainment, articulation)	4	4	16	• Robust strategic planning • Effective environmental scanning • Strong partnerships • Clear links between strategy and practice • Concerted demands for increased activity levels	4	1	4	• Robust monitoring via ROA • Clear performance metrics • Amendment of strategic direction/plans • Rolling curriculum review	Board, ELT BoM
1.2	College may be disadvantaged by changes to either UK or Scottish Government policies	4	3	12	• Effective environmental scanning • Negotiation/influence at national level	4	2	8	• Review of changes and amendment of strategic direction/plans • Financial strategy sensitivities	ELT BoM
1.3	College disadvantaged by changes arising from UK leaving European Union	3	4	12	• Negotiation/influence at national level • Review of activities/ projects • Responsiveness to new opportunities	2	2	4	• Review of changes and amendment of strategic direction/plans/ curriculum • Financial strategy not ESF dependent	ELT BoM

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Post Holders							
	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility/ Committee Oversight
2	**Financial**									
2.1	Change in SFC Funding Methodology and Allocation – Reduction in Funding	3	3	9	• Negotiation/influence at national level • Contingency plans for reduced funding	2	3	6	• Advance modelling of new funding methodologies and allocations • Monitoring impact of changes • Amendment of strategic or operational direction/plans • Financial strategy sensitivities	ELT F&GP
2.2	Failure to achieve institutional sustainability	5	4	20	• Protection of funding through dialogue with SFC • Robust annual budget-setting and multi-year financial strategic planning (from 2018-19) • Effective budgetary control • Where required, swift action to implement savings	4	3	12	• Regular monitoring of budgets • Regular review of financial strategy and non-core income sensitivity	CLT F&GP
2.3	Salary and conditions of service pressures outstrip ability to pay	4	4	16	• Influence within Employers Association • Management of staffing expenditures	4	3	12	• Expenditure modelling • On-going discussions with staff • Financial strategy sensitivities	ELT HoHR F&GP

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Post Holders							
	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility/ Committee Oversight
2	**Financial (cont.)**									
2.4	Financial Fraud	4	3	12	• Strong financial controls: segregation of duties and review of transactions • Review of impact of any changes in structure or duties • Whistleblowing arrangements	3	2	6	• Continuous review of financial controls • Internal Audit programme	HoF Audit
2.5	Scotland's Colleges Foundation refuses/withholds funding for key College priorities	5	3	15	• Only £25,000 of unallocated funds remain. Appropriate bid arrangements in place	3	2	6	• Monitor and advise Board of Management	HoF F&GP
2.6	Failure to achieve credit (activity) target	5	3	15	• Real time monitoring system • Identify & implement additional/alternative provision where required	4	1	4	• Continuous review of progress v targets. Current shortfall of approx. 450 credits – expected to achieve target, including ELC target	ELT HoC HoP&Q F&GP
2.7	Insufficient Student Support Funding to meet demand.	4	5	20	• Strong financial monitoring • Possible opportunity to request additional in year funding	4	2	8	• Continuous monitoring of demand v funding allocation • Ongoing dialogue with Scottish Funding Council. Confirmation received from SFC that full amount of additional funding requested would be allocated	PRIN HoF F&GP

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Post Holders							
	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
3 Organisational										
3.1	Legal actions; serious accident; incident or civil/criminal breach	4	5	20	• Adherence to legislative and good practice requirements • Positive Union relations and staff communication • Effective management development programmes	3	2	6	• Monitoring and reporting in key areas – eg H&S, equalities, employee engagement • Continuous professional development • Internal audit programme • Staff surveys	ELT BoM
3.2	Reputational Risk – Loss of reputation with key stakeholders	4	3	12	• Marketing strategy • Positive marketing approaches	4	2	8	• Stakeholder engagement • Social media monitoring arrangements	PRIN VPBD&CS HoP&Q BoM
3.3	Disasters – eg Fire, MIS Failure, Failure of Emergency Procedures	5	4	20	• Sound systems of administration • Clear fire and disaster recovery arrangements • Staff CPD	5	1	5	• Business Continuity Plan including scenario testing	VPBD&CS VPL&S HoCS BoM
3.4	Failure to meet Prevent and related obligations	5	3	15	• Prevent training • Staff awareness and contingency planning • Engagement/practice sharing with local agencies	5	1	5	• Business Continuity Plan including scenario testing • Information sharing with local agencies	VPBD&CS HoCS **BoM**

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Post Holders							
	Board	Board of Management	HoC	Head of Curriculum	HoSS&G	Head of Student Support & Guidance
	ELT	Executive Leadership Team	HoP&Q	Head of Planning & Quality		
	CLT	College Leadership Team	HoF	Head of Finance		
	PRIN	Principal	HoHR	Head of Human Resources		
	VPL&S	Vice Principal Learning & Skills	HoBD	Head of Business Development		
	VPBD&CS	Vice Principal Business Development	HoCS	Head of Corporate Services		

Score	Impact	Likelihood
1	Routine	Remote
2	Minor	Unlikely
3	Significant	Possible
4	Major	Probable
5	Critical	Very likely

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
3	**Organisational (cont.)**									
3.5	Industrial Relations Problems (including industrial action)	4	5	20	• Adherence to legislative and good practice requirements • Positive Union relations and staff communication • Effective management development programmes • Industrial action continuity planning		5	20	• Regular union/management dialogue • Regular employee engagement monitoring • Open communication with staff • EIS currently taking industrial (including strike) action.	ELT HoHR HR
3.6	Failure to achieve ambitions of ICT strategy; strategy and development is ineffective	4	4	12	• Planning, careful phasing of changes to processes and systems • Effective management of ICT arrangements	4	2	8	• Regular review/reporting on milestones, systems effectiveness etc • Regular CPD	VPBD&CS HoCS Audit
3.7	Breach of ICT/Cyber security	4	3	12	• Effective management of ICT arrangements • Active ICT/data security monitoring and cyber security policy	4	2	8	• Staff CPD on cyber security issues • Regular security monitoring/testing • Cyber resilience plan	VPBD&CS HoCS Audit

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
3 Organisational (cont.)										
3.8	Breach of data security/data protection	5	4	20	• Effective management of ICT arrangements and GDPR compliance • Mandatory staff CPD and awareness raising on data protection (relative to role)	4	2	8	• Active data protection monitoring and auditing • Effective information and data security policies in operation • Regular data security monitoring/testing • GDPR Action Plan	VPBD&CS, HoCS Data users Audit
3.9	Failure to reach aspirational standards in learning, teaching and service delivery	4	3	12	• Clear quality arrangements and priority actions • Continuous self-evaluation and action planning • Rigorous CPD arrangements in place • Regular classroom observation and learner feedback arrangements	4	3	12	• Comprehensive monitoring of key PIs and student/staff feedback • Regular Stop and Review events • External review and validation findings • Current PI report indicates no significant improvement in retention at this moment	VPL&S, VPBD&CS HoP&Q HoC L&T
3.10	Failure to achieve/maintain compliance arrangements, eg contracts; awarding bodies; audit	4	3	12	• Robust strategic planning and monitoring • Effective environmental scanning • Strong partnerships • Clear links between strategy and practice	2	2	4	• Effective internal monitoring/review/verification arrangements • External review findings	PRIN CLT Audit

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk

Risk Number	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility /Committee Oversight
3 Organisational (cont.)										
3.11	Failure to meet the deadlines in our successful bid to SoSEP regarding the provision of Hub and Spoke model for Engineering, Construction and Care	3	4	12	• Robust project planning in place and feedback via EMT to Board of Management • Clear and consistent approach to the project with Borders College • Independent scrutiny through clerk of works (for building works) • SFC involvement at all stages of the project	3	3	9	• Curriculum development planning through L&T Committee • Overall project through regular Board of Management updates • Further scrutiny through SoSEP Board	PRIN VP BD&CS VP L&S BoM
3.12	Failure to reach contractual agreement with CITB regarding delivery of Construction related Apprenticeships	4	4	16	• National issue, discussions with CITB, SQA now escalated to include SDS and Scottish Government • Request to defer new qualification until 2019/20 being considered by SQA regulatory body	4	4	16	• Principal actively involved in national discussions • Detailed scenario planning regarding costs of delivery and impact on college currently being completed • Curriculum Manager involved in national forum exploring options	PRIN VP L&S CM BoM

Key to Risk Estimation/Score based on scale of 1 – 5 for impact/likelihood: Green (1-8) = Minor Risk; Amber (9-15) = Significant Risk; Red (16-20) = Major Risk; Purple, (>21 - 25) = Fundamental Risk