University of the Highlands and Islands
Moray College

Meeting of Audit Committee
On Thursday 7 October 2021
At 1330 by Teams
A G E N D A

Number	Item	Presented By	Action Required: Decision, Discussion, For Noting
A.21.03.01	(i) Resignations	Clerk	Noting
	(ii) Appointments		
A.21.03.02	Apologies for Absence	Clerk	Noting
A.21.03.03	Any Additional Declarations of Interest including specific items on this Agenda	Convenor	Noting
A.21.03.04	Draft Minutes of Audit Committee meeting held on 18 May 2021*	Convenor	Decision
A.21.03.05	Draft Matters Arising from Audit Committee meeting held on 18 May 2021 *	Clerk	Noting
A.21.03.06	Review of Risk Register	Shelly	Noting/Discussion
	(i) Current Risk Register and Mitigating Actions		
	(ii) Update on status re planning for achieving carbon neutrality		
A.21.03.07	Internal Audit Matters	Shelly/Wylie Bisset	Noting/Discussion/ Decision
	(i) Update on Complaints Handling		
	(ii) Status of remaining plan for 2020/21		
	(iii) Internal Audit Plan for 2021/22		
A.21.03.08	Review of Audit Register	Shelly	Noting
A.21.03.09	External Audit: Plan for Annual Audit by EY for AY 2020/21	EY	Noting
	(i) Matters Arising, any RSB/ SFC implications		

	(ii) Letter from EY to those charged with Governance		
A.21.03.10	Fraud	Shelly	Noting
	(i) Annual paper on Fraud		
A.21.03.11	Cyber Security - RESERVED	Derek	Discussion/ Noting
	(i) Matters arising from Cyber incident		
	(ii) Development of an Assurance Framework for the Committee		
	(iii) GDPR Update		
A.21.03.12	College Policies		
	(i) Status of all College Policies, Plan for Review and Updating	Derek	Noting
	(ii) Approval of amended Fraud Policy	Shelly	Decision
A.21.03.13	Emerging Issues	Convenor	Noting
	(i) UHI Audit Committee Chairs' Meeting – 10 November 2021		
	(ii) Committee Evaluation		
	(iii) Committee Annual Report to the Board		
	(iv) Retirement of Clerk and appointment of replacement		
RESERVED ITEMS			
A.21.03.14	Draft Reserved Minutes of Audit Committee held on 18 May 2021*	Convenor	Decision
A.21.03.15	Reserved Matters Arising from Audit Committee held on 18 May 2021*	Clerk	Noting
A.21.03.16	Date of Next Meeting of Audit Committee – 25 November 2021	Clerk	Noting
A.21.03.17	Possible date of Joint Audit Committee and Finance and General Purposes Committee – 17 February 2022	Clerk	Noting

BOARD OF MANAGEMENT
Audit Committee
Draft Minutes of Meeting
Held on
Tuesday 18th May 2021
At 13.30 by Teams

Present :	J McLeman	Convenor
	D McKinstrey	
	K Gee	
In attendance:	S McInnes	
	Stephen Reid	Ernst & Young – External Auditors
	S McCready	Wylie & Bisset LLP – Internal Auditors
	D Duncan	
	E Melton	Clerk

		ACTION	DATE
A.21.03.01	**Resignations and Appointments**		
1.1	There were no resignations or appointments		
A.21.03.02	**Apologies for Absence**		
2.1	Apologies for absence had been received from Cathie Fair.		
A.21.03.03	**Any Additional Declarations of Interest including specific items on this Agenda**		
3.1	There were no additional declarations of interest		
A.21.03.04	**Draft Minutes of Joint Audit and Finance & General Purposes Committee meeting held on 11 February 2021**		
4.1	The minutes were accepted as a true and accurate record and approved by the Committee: Proposed: D McKinstrey Seconded: K Gee		
A.21.03.05	**Draft Minutes of Audit Committee meeting held on 16 February 2021**		
5.1	The minutes were accepted as a true and accurate record and approved by the Committee: Proposed: D McKinstrey Seconded: K Gee		
A.21.03.06	**Draft Matters Arising of meetings held on 11 and 16 February 2021**		
6.1	11 February 2021 – Most actions were noted as complete, some were discussed on the agenda and a number were carried over, the status as set out in the list of actions arising.		
6.2	16 February 2021 -		
	It was agreed that item A.21.03.08 be discussed next due to S McReady possibly having to leave early.		
A.21.03.08	**Internal Audit Reports**		
8.1	**(i) Board Effectiveness Review**		

	The report had been accepted by the Board in March for submission to SFC. It was queried whether the submission had been made due to Mrs Fair's absence.		
ACTION	Convenor to follow up with the Principal to determine whether the report had been submitted to the SFC. If not, an addendum/ covering note might be needed to contextualise actions due imminently and unable to be progressed to illness;	Convenor	Immediate
ACTION	To add the actions arising from the Board Effectiveness Report to the Audit Register; and to determine status of action on support Staff recruitment to the Board.	S McInnes D Duncan	Immediate
	It was noted that a further discussion may be needed to set a plan going forward if Mrs Fair is not due to return to work in the near future.		
8.2	(**ii) Budgetary Controls** S McReady presented the report, highlighting significant points throughout and explaining the layout. The report concluded that Moray College was awarded the highest outcome of 'strong' with good practice points noted. There were three 'low' grade recommendations and one observation. In terms of the sample size, Mr McReady commented that would have been extended if the responses had indicated. J McLeman advised that the updated Financial Regulations Procedure should be presented to the Finance & General Purposes Committee rather than Audit Committee. D McKinstrey had noted that the report states there had been 3 contributing factors to the shortfall, however, only the pandemic was mentioned. S McInnes explained that the reduction in student intake and lack of funding for national bargaining were the other 2. The committee accepted the recommendations as set out.		
8.3	**(iii) Leadership of Learning & teaching by Promoted lecturers** S McReady supported the report. The report provides a detailed background with a 'strong' level conclusion being reached, with 2 'low' grade recommendations.. The recommendations were discussed and accepted. D McInstrey questioned, with N Yoxall leaving Moray College, whether recommendation 1 is at risk of not being completed? D Duncan explained that the recruitment process has started for a replacement although he did not believe that N Yoxall would leave the action incomplete.		
8.4	**(iv) Update on plan for 2020/21**		

	Audit of complaints handling arrangements; The proposal is to review complaints handling. S McInnes and S McReady had discussed and agreed the change from estates to complaints handling. S McReady explained the review will be look at all aspects, including staff, students and external providers; policies, procedures in place; actions taken including communications, recurring themes; and reporting. The red button process will also be looked at although D Duncan mentioned that this was managed via UHI. The Convenor asked if the audit could include arrangements for handling particularly sensitive matters and that was confirmed. The proposal was agreed. Mr McReady confirmed that the overall plan allowed for the closure of audit actions by WB.		
ACTION	D Duncan to double check the proposed fieldwork dates of 19 July and confirm with S McReady.	D Duncan	
A.21.03.09	**Review of Audit Register**		
9.1	S McInnes supported the paper provided advising there are no items to close of currently. There are 4 items that S McInnes suggests being rolled forward with revised dates, mainly due to the Covid-19 situation. Re the H&S action, J McLeman commented that it would be helpful to note on the register where curriculum areas are assessed for H&S as they are open up. It was noted that the UHI risk register action has a revised date of 31 December although this is not a confident date. J McLeman queried the proposed revised dates for the procurement actions, given the length of time these had been open. S McInnes explained that the procurement staff member had recently resigned, APUC will now provide a full-time member of staff based at Moray College, to be appointed. It was requested this action date be brought forward to 30 November 2021.		
ACTION	S McInnes to adjust audit action completion dates as per discussion, and to add to the register the actions from all the above reports.	S McInnes	ASAP
A.21.03.07	**Review of Risk Register**		
7.1	**(i) Current Risk Register and Mitigating actions** S McInnes directed members to the covering paper which highlights significant amendments to the register. Amendments have been made considering comments from the Board and Audit Committee. In summary, the overall level of risk is lower compared to the previous version reviewed by the Committee. There is better news around the financial situation with everything looking slightly better which is a definite positive and that had informed some of the changes.		

	D McKinstrey felt there had been more of a drive to reduce the 'red' risks and sought assurances that this had been done with confidence. Also, it would be good to see some more narrative on risks rather than just a covering paper. Risk on commercial income has been downgraded as funding was higher than anticipated, and the target for this year had been met, noting this is a snapshot in time. J McLeman queried the assessment of commercial risk, which combined furlough income/commercial activities, and would have more confidence on sight of the commercial plan, which has not been shared.		
ACTION	Convenor to raise the matter of the Commercial Plan at the Board.	Convener	June 2021
	There was discussion about the structure of the risk register, as some risks seem effectively to be subsets of higher risks. D McKinstrey suggested that e.g. the top 10 risks be identified with related risks noted as in a parent-child relationship, although this would be a decision for SLT. J McLeman noted that the description of some risks felt a bit 'tired' and described past eventualities rather than being updated for the current context. S McInnes agreed she would be comfortable revisiting the risk register, and now is the right time to do so particularly in view of the work being done on the strategy. J McLeman noted that the Board Risk Workshop in the summer is still an open action and consideration will have to be given on how best to structure that to have an effective workshop.		
ACTION	Discuss with SLT options for alternative approaches to the risk register, and, as part of the consideration, confer with Academic Partners regarding their practices.	S McInnes	Next Audit Committee meeting
7.2	**(ii) Follow up on Climate Change and achieving Carbon Neutrality** There was discussion as to whether this item should be on the risk register, in view of the long-term planning implications in meeting the obligation. All agreed it should be. D Duncan added that there is now government funding being made available to undertake an audit. J Mcleman advised this question had also been raised and discussed at the UHI Audit Chairs meeting.		
ACTION	Climate change and achieving carbon neutrality to be added to the Risk Register.	S McInnes	ASAP
A.21.03.10	**External Audit: Scope and Plan for Annual Audit for AY 2020/21**		

10.1	Mr Reid explained the process that the plan is usually presented to the committee before being submitted to Audit Scotland. This is EY's 5th year as external auditors, now extended to a 6th due to the pandemic. There will be two aspects to the audit namely the financial statements audit and the wider scope audit. The key financial statement risks are as in previous years, namely risk of fraud, and inherent risk related to valuation of property and assets, pension assets and liabilities. The wider scope audit will consider the financial position and arrangements for securing financial sustainability; and the suitability and effect of corporate governance arrangements. The wider scope risks relate to medium term financial planning. NB; the planning materiality of c2% of forecast expenditure for the year has been reinstated. There will a similar approach as in previous years with regards to reporting to the committee and areas for focus. Throughout the process, EY will consider the issues faced during the pandemic and any funding received. The timetable is yet to be finalised, and EY are also awaiting communication on any extension of deadlines. The finalised timetable will be agreed with management with a finalised plan reported. The committee will continue to plan on the usual approach of a joint meeting with the F&GP at the end of the year, for approval at the subsequent Board in December, noting that this may change. Due to the audit plan not being included in the Committee pack, it was requested that any further comments or questions should be communicated to S Reid via email, copy the Convenor.		
ACTION	To keep the external audit timetable under review and to advise the Committee of the finalised audit plan.	S McInnes/S Reid	Next Audit Committee
ACTION	External Annual Audit Plan to be circulated to committee members, requesting any comments to be provided by 27 May 2021 cc J Mcleman.	E Melton	Immediate
A.21.03.11	**OSCR Return: Status of College's 2021 Annual OSCR Return**		
11.1	S McInnes confirmed this return has been completed and submitted to OSCR on time.		
A.21.03.12	**National Fraud Initiative**		
12.1	**(i) College Return for 2021** **(ii) Review of Committee Input** A summary report on data matches found and results of analysis was provided to the committee. All were cleared with no suggestion of fraud identified.		

	D McKinstrey questioned whether individuals identified as being a match to returns at Companies House are compared to the declarations of interest held by the College, including previous matches. S McInnes confirmed that staff have to disclose external interests, and any paid employment has to be agreed by the principal, but the matches identified had not been compared to the declarations of interests.		
ACTION	Update National Fraud Initiative process such that relevant matches will be cross referenced with the register of disclosed interests.	S McInnes	Update the process by next meeting
	More generally, D McKinstrey queried if the activities and findings under the NFI exercise are reported to staff for their awareness, whether there a briefing beforehand with an update on completion. Following discussion, it was agreed that this be considered further, and the Committee advised of the outcome.		
ACTION	Shelly to consider what staff communications, if any, might be appropriate to advise on activities undertaken under the NFI initiative.	S McInnes	Next meeting
	Part A question 3 of the Appendix asks if the organisation has considered real time matching. J McLeman asked if the College had considered this approach.		
ACTION	Shelly to consider the option of real time matching and follow up, and the implications for the College, report at next meeting.	S McInnes	7/10/2021
	Scott McReady left meeting at 15.19pm		
A.21.03.13	**Cyber Security**		
13.1	**(i) Framework for ongoing assurance to the committee** D Duncan outlined that there has been considerable learning and discussions following the cyber incident. A high-level report is to be completed and circulated round Academic Partners. Clearance is being sought for circulation to Board members. The intention is for there to be a partnership approach to cyber security going forward. D Duncan will be Moray College's representative on the committee addressing cyber security. J McLeman also advised that a high level 'lessons learned' report had been discussed at the UHI Audit Chairs Committee, with the intention of providing such a report in June. There was discussion as to how the Audit Committee can gain assurance in relation to cyber security matters, such that the board of Moray College can be assured. The material circulated to the Committee in advance set out approaches to		

	an assurance framework, which seemed to provide a good standardised starting point. This could sit alongside/ align with a wider UHI framework. Members questioned how the board can gain assurances that Moray's responsibilities are adequately addressed alongside UHI's activities. A framework should indicate where roles and responsibilities lie within UHI and partners, such that matters can be identified and performance monitored and reported. It was noted this approach may need to be iterative.		
ACTION	Consider how an assurance framework can be developed for Moray College to align with a UHI framework, so that the Committee can monitor and to provide assurance to the Board. Proposals to be provided to the next meeting of the Committee.	D Duncan	Next meeting
	D Duncan provided the committee with a brief update on the cyber incident, currently in the phase of lessons learned although there are still ongoing issues with some systems still being affected. Data files are currently in the process of being migrated on to SharePoint to comply with the new records management policy. The framework being developed covers both technology and data. He explained the recovery process and ICT use going forward, although full assurances will be laid out within the framework.		
ACTION	John Maher to be invited to next meeting of Audit Committee	D Duncan/E Melton	
A.21.03.14	**College Policies**		
14.1	**(i) Status of all College Policies, Plan for review** Unfortunately, there is no access to policies due to the cyber incident. There is now a backlog of policies to be reviewed, due to policies being rescheduled and a new CCTV system being installed, which will also require an update to policies. As already actioned, D Duncan to present status and plan to next meeting of the Audit Committee.		
ACTION	Convenor to advise on current situation at next Board meeting.	**Convenor**	**June 2021**
14.2	**(ii) Approval of amended fraud Policy** The policy was unavailable, and the updated version will be circulated by S McInness on availability to the Committee for approval, as already actioned		
A.21.03.15	**Emerging Issues**		
15.1	**(i) Feedback from UHI Audit Committee Chairs Meeting** J McLeman provided an update on matters throughout the meeting including the cyber incident and climate change agenda items.		

	One further agenda item had been discussed, namely a reminder from EO of the requirement in the Financial Memorandum for Academic Partners to obtain annually an internal audit opinion, and for that to be reported to UHI/ SFC through the year end reporting process. The template for assurance reports from Audit Committees to Boards also called for Audit Committees to comment on the quality of internal audit work carried out. In the discussion, there was a query as to the take-up of value- added options offered by WB as part of the award of contract process. Shelly to follow up.		
ACTION	Shelly to follow up on the take up of value-added options proposed by WB.	S McInnes	Next audit committee
15.2 **ACTION**	**(ii) Status of Committee Evaluation** This is currently ongoing. Current status to be discussed with D Patterson.	 S McInnes	
15.3	**(iii) UHI wide considerations impacting Audit Committee work** There is no specific update at the moment although it is thought that work on shared services will be moving forward.		
RESERVED ITEMS			
A.21.03.16	**Draft Reserved Minutes of Joint Audit and Finance & General Purposes Committee meeting held on 11 February 2021**		
16.1	This item is Reserved and the Minute held on Confidence.		
A.21.03.17	**Draft Reserved Minutes of Audit Committee held on 16 February 2021**		
17.1	This item is Reserved and the Minute held on Confidence.		
A.21.03.18	**Draft Matters Arising of Audit Committee meetings held on 11 and 16 February 2021**		
18.1	This item is Reserved and the Minute held on Confidence.		
A.21.03.19	**Update on Cyber Incident**		
19.1	This item is Reserved and the Minute held on Confidence.		
A.21.03.20	**Date of New Meeting**		
20.1	7 October 2021		
	Meeting closed at 16.05pm		

Matters Arising from Audit Committee 18 May 2021

		ACTION	DATE	Update
A.21.03.06	**Matters Arising/Action Sheet from Audit Committee meeting held on 16 February 2021**			
6.1	6.2.1 - To suggest a Risk Workshop take place prior to June or Sept [2020] Board meeting – remains open. Jessie to speak to Peter. Following discussion, it was felt not to be appropriate to hold a Risk Workshop by Teams but to plan for one in Spring, or as can be arranged.	J McLeman	Remains open	Jessie has raised with Peter
6.2	11.1.2 - status of review of college policies; In the meantime, to circulate the paper to all Convenors	C Fair	Immediate	Completed
6.3	8.2.2 - Re addressing carbon neutrality, D Duncan to follow up on the areas set out in the paper with a view to developing an approach and a plan, and to update the Committee on the status at its meeting in October 2021.	D Duncan	October 2021 Audit Committee	
	External Audit			
6.4	10.1 - The Committee asked that relevant risks be shared with other appropriate Committees on an on-going basis.	C Fair	ASAP as required	Remains open
	GDPR Update			
6.5	12.1 - D Duncan to update the Committee annually in October in relation to GDPR, unless there are any exceptions or serious incidents which should be reported immediately. The Committee could also review cyber security matters as part of the same report, approach to be confirmed following Board discussion.	D Duncan	October 2021 Audit Committee	On Agenda
A.21.03.07	**Review of Risk Register**			
	(i) Current Risk Register and Mitigating actions			
7.1.1	Convenor to raise the matter of the Commercial Plan at the Board.	Convener	June 2021	the matter was raised by the Convenor at the June Board - and the notes now capture that. The plan is to be outlined at the October Board and the details presented to the December Board.

7.1.2	Discuss with SLT options for alternative approaches to the risk register, and, as part of the consideration, confer with Academic Partners regarding their practices.	S McInnes	Next Audit Committee meeting	
	(ii) Follow up on Climate Change and achieving Carbon Neutrality			
7.2	Climate change and achieving carbon neutrality to be added to the Risk Register.	S McInnes	ASAP	
A.21.03.08	**Internal Audit Reports**			
	(i) Board Effectiveness Review			
8.1.1	Convenor to follow up with the Principal to determine whether the report had been submitted to the SFC. If not, an addendum/ covering note might be needed to contextualise actions due imminently and unable to be progressed to illness;	Convenor	Immediate	Report has been submitted
8.1.2	To add the actions arising from the Board Effectiveness Report to the Audit Register; and to determine status of action on support Staff recruitment to the Board.	S McInnes D Duncan	Immediate	
	(iv) Update on plan for 2020/21			
8.4	D Duncan to double check the proposed fieldwork dates of 19 July and confirm with S McReady.	D Duncan	Immediate	
A.21.03.09	**Review of Audit Register**			
9.1	S McInnes to adjust audit action completion dates as per discussion, and to add to the register the actions from all the above reports.	S McInnes	ASAP	
A.21.03.10	**External Audit: Scope and Plan for Annual Audit for AY 2020/21**			
10.1	To keep the external audit timetable under review and to advise the Committee of the finalised audit plan.	S McInnes/S Reid	Next Audit Committee	
10.2	External Annual Audit Plan to be circulated to committee members, requesting any comments to be provided by 27 May 2021 cc J Mcleman.	E Melton	Immediate	
A.21.03.12	**National Fraud Initiative**			
12.1	Update National Fraud Initiative process such that relevant matches will be cross referenced with the register of disclosed interests.	S McInnes	Update the process by next meeting	
12.2	Shelly to consider what staff communications, if any, might be appropriate to advise on activities undertaken under the NFI initiative.	S McInnes	Next meeting	
12.3	Shelly to consider the option of real time matching and follow up, and the implications for the College, report at next meeting.	S McInnes	7/10/2021	
A.21.03.13	**Cyber Security**			
	(i) Framework for ongoing assurance to the committee			
13.1	Consider how an assurance framework can be developed for Moray College to align with a UHI framework, so that the Committee can monitor and to provide assurance to the Board. Proposals to be provided to the next meeting of the Committee.	D Duncan	Next meeting	On Agenda for discussion
13.2	John Maher to be invited to next meeting of Audit Committee	D Duncan/E Melton	Immediate	Remains open

A.21.03.14	**College Policies**			
	(i) Status of all College Policies, Plan for review			
14.2	Convenor to advise on current situation at next Board meeting.	Convenor	June 2021	Advised at June Board
A.21.03.15	**Emerging Issues**			
	(i) Feedback from UHI Audit Committee Chairs Meeting			
15.1	Shelly to follow up on the take up of value-added options proposed by WB.	S McInnes	Next audit committee	
	(ii) Status of Committee Evaluation			
15.2	This is currently ongoing. Current status to be discussed with D Patterson	S McInnes	Immediate	

Wylie Bisset
Chartered Accountants, Business & Tax Advisers

University of the Highlands and Islands
Moray College
Oilthigh na Gàidhealtachd agus nan Eilean
Colaiste Mhoireibh

Moray College UHI

Internal Audit Plan

2021 - 2022

August 2021

Table of contents

1. Introduction

Background
Wylie & Bisset LLP were appointed as Internal Auditors by the Board of Management with effect from 1 August 2020 for a period of 2 years until 31 July 2022 with the option to extend for 2 further 12-month periods.

Internal Audit
In accordance with Moray College UHI ("the College") Financial Memorandum with the Scottish Funding Council("the Council") the Board of Management is required to secure the provision of an effective Internal Audit Service (IAS). The prime responsibility of the IAS is to provide the Board of Management, the Principal and other Senior Management of the College, with an objective assessment of the adequacy and effectiveness of management's internal control systems.

The IAS objectively examines, evaluates and reports on the adequacy of internal control thus contributing to the economic, efficient and effective use of resources and to the reduction of the potential risks faced by the College. Also, the operation and conduct of the IAS must comply with the guidelines set down by the Chartered Institute of Internal Auditors and Public Sector Internal Audit Standards.

Terms of Reference – Internal Audit
The provision of the IAS by Wylie & Bisset LLP is covered by the letter of engagement dated 6 November 2020.

Preparation of Plan
The original Audit Needs Assessment was approved by the Audit Committee on 24 November 2020. This document covers the Plan for 2021/22 and was developed following discussions with the Chair of the Audit Committee and the Director of Finance. During our discussions, it was proposed that the reviews of the SITS System, Cyber Security, Estates Strategy and Working from Home Arrangements are undertaken during 2021/22 and reviews of the Moray Growth Deal, Course Costing, Curriculum Planning noted as potential areas for review for future years.

Formal Approval
The plan will be presented to the Audit Committee of the College for approval on 7 October 2021.

2. Operational Plan 2021/22

Audit Area	High level indicative summary scope	Total Number Of Days
SITS Systems	The purpose of this assignment is to review the use of the SITS System at the College. We will look to ensure that the system is operational and assess whether the College are using the system to its full potential. We will also assess management of the system and look to ensure that College staff have had appropriate training on the system.	5
Income Collection & Credit Control	The purpose of this review is to ensure that the arrangements in respect of income collection and credit control are appropriate and are operating effectively and efficiently including restaurant and refectory income. This review will provide assurance to the Board, via the Audit Committee, that the College's financial controls are adequate. We will also consider the communication and reporting between the College and UHI regarding income funds.	4
Cyber Security	We will review the overall IT systems in place to ensure the appropriate controls are in place and that these are operating as expected. The review will specifically examine the specifications and systems operated by the College to ensure that they are fit for purpose. We will also focus on reviewing network security arrangements in place to verify that users, data, and devices are sufficiently protected from cyber threats. We will also consider the enhancements made to the security arrangements following the cyber incident. We note that our review will only focus on areas of IT that are the College's responsibility, and not areas that are the responsibility of UHI.	5
Estates Strategy	The purpose of this assignment is to review the development of the College's Estates Strategy. We will review the Strategy and benchmark this against our other clients to ensure that the Strategy considers areas that we would expect to be included.	4
Working from Home Arrangements	We will also review the Working from Home (WFM) arrangements in place at the College. We will consider whether the College has undertaken risk assessments of staff members work space and that this is monitored by the College. We will also consider the arrangements put in place to support home working arrangements following the relaxation of Covid-19 restrictions.	4

2. Operational Plan 2021/22

Audit Area	High level indicative summary scope	Total Number Of Days
Implementation and Use of Brightspace	We will review the implementation of the new Brightspace system that is operational at the College to assess whether the systems are working as anticipated and that the College is fully utilising the benefits and efficiencies that the new systems offer.	5
SSF Audit	Mandatory review of the Student Support Funds Returns.	2
EMA Audit	Mandatory review of the Education Maintenance Allowance Returns.	1
Credits Audit	Mandatory review of the Credits Return.	2
Follow Up Review	This will be an ongoing review undertaken throughout the year to assess whether the College has appropriately implemented the internal audit recommendations made in 2020/21 and earlier years. Our ongoing review will consider whether any issues are outstanding beyond the agreed implementation deadlines. Our ongoing review will consider all outstanding recommendations to provide the Audit Committee with independent assurance that we are satisfied that these recommendations have been fully implemented by the College and can therefore be removed from the rolling audit action plan.	2

2. Operational Plan 2021/22 (cont'd)

Assignment Plans

A detailed assignment plan will be prepared for each audit undertaken, setting out the scope and objectives of the work, allocating resources and establishing target dates for the completion of the work. Each assignment plan will be agreed and signed off by an appropriate sponsor from the College.

Key Dates

Visit	Audit Areas	No. of Audit Days	Key College Personnel	Provisional Date for Visit	Date of Issue of Draft Report	Provisional Date for Reporting to the Audit Committee
Visit 1	Working from Home Arrangements	4	Derek Duncan	9 December 2021	24 December 2021	17 February 2022
Visit 2	SITS System Income Collection & Credit Control	5 4	Shelly McInnes & Derek Duncan Shelly McInnes	28 March 2022	14 April 2022	May 2022
Visit 3	Cyber Security	5	Derek Duncan	4 April 2022	22 April 2022	May 2022
Visit 4	Estates Strategy Implementation and Use of Brightspace	4 5	Derek Duncan Shelly McInnes & Derek Duncan	18 July 2022	5 August 2022	October 2022
Visit 5	EMA Audit SSF Audit Credits Audit	1 2 2	Derek Duncan Derek Duncan Derek Duncan	12 September 2022	23 September 2022	October 2022
	Follow Up	2	Shelly McInnes	Quarterly	N/A	Various

Appendix A – Summary of Internal Audit Input

1 August 2020 to 31 July 2023		Operating Plan (No. Of days)			Potential Audit Areas
System	**Audit Area**	**2020/21**	**2021/22**	**2022/23**	
Financial Systems	Budgetary & Financial Reporting	4			
	Income Collection & Credit Control		4		
	Purchasing & Payments			4	
	Procurement			5	
	Course Costing				*
Staff	Leadership of Learning & Teaching by Promoted Lecturers	7			
	Staff Wellbeing & Mental Health				*
	Working from Home Arrangements		4		
Students	Curriculum Planning				*
	Student Retention			4	
Operational	Policy Awareness				*
	Complaints Handling	4			
	Health & Safety				*
	Estates Strategy		4		
	Commercial Strategy				*
Systems	Implementation and Use of Brightspace		5		
	SITS System		5		
	Cyber Security		5		*
	Business Continuity Planning				*
	Carried Forward	**15**	**27**	**13**	

Appendix A – Summary of Internal Audit Input

1 August 2020 to 31 July 2023		Operating Plan (No. Of days)			Potential Audit Areas
System	**Audit Area**	**2020/21**	**2021/22**	**2022/23**	
	Brought Forward	**15**	**27**	**13**	
Corporate Affairs & Governance	Board Effectiveness	7			
	Risk Management			4	
	Corporate Planning, Monitoring & KPIs				*
	Moray Growth Deal				*
Mandatory	Credits Audit	2	2	2	
	SSF Audit	2	2	2	
	EMA Audit	1	1	1	
Required	Follow Up review	2	2	2	
	Audit Management	4	4	4	
	Total Days	**33**	**38**	**28**	

We have added a column headed up 'potential audit areas'. These were areas that arose through discussions with the Chair of the Audit Committee, Principal and Director of Finance however due to the budgeted internal audit days being 33 days per annum, we have been unable to fit these within the original 3 year plan. We note that we have brought forward audit days from 2022/23 to 2021/22 to incorporate the reviews discussed at the 2021/22 planning meeting.

Appendix B – Grading Structure

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

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

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

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

Analysis of Performance Indicators

Performance Indicator	Target
Internal audit days completed in line with agreed timetable and days allocation	100%
Draft scopes provided no later than 10 working days before the internal audit start date	100%
Draft reports issued within 20 working days of exit meeting	100%
Management provide responses to draft reports within 15 working days of receipt of draft reports	100%
Final reports issued within 10 working days of receipt of management responses	100%
Recommendations accepted by management	100%
Draft annual internal audit report to be provided by 31 August each year	100%
Attendance at Audit Committee meetings by a senior member of staff	100%
Suitably experienced staff used on all assignments	100%

Ernst & Young LLP
Atria One
144 Morrison Street
Edinburgh
EH3 8EX

Tel: + 44 131 777 2000
Fax: + 44 131 777 2001
ey.com

Members of the Audit Committee
Moray College UHI
Moray Street
Elgin
IV30 1JJ

7th September 2021

Ref: SR/GS
Direct line: 0131 777 2839
Email: SReid2@uk.ey.com

Dear Audit Committee Members,

External audit: Year ending 31 July 2021

Auditing standards require us to formally update our understanding of your arrangements for oversight of management processes and arrangements annually. I am therefore writing to ask that you please provide a response to the following questions.

1. How does the Audit Committee, as 'those charged with governance' at Moray College ("the College"), exercise oversight of management's processes in relation to:

    - undertaking an assessment of the risk that the financial statements may be materially misstated due to fraud or error (including the nature, extent and frequency of these assessments);
    - identifying and responding to risks of fraud in the College, including any specific risks of fraud which management has identified or that have been brought to its attention, or classes of transactions, account balances, or disclosures for which a risk of fraud is likely to exist;
    - communicating to employees its view on business practice and ethical behaviour, for example by updating, communicating and monitoring against the College`s code of conduct;
    - encouraging employees to report their concerns about fraud; and
    - communicating to you the processes for identifying and responding to fraud or error?

2. How does the Audit Committee oversee management processes for identifying and responding to the risk of fraud and possible breaches of internal control?

3. Have there been any significant changes in the design and/or operating effectiveness of management controls as a result of the Coronavirus outbreak?

4. How do those charged with governance assure themselves that the furloughing of staff has not adversely impacted the segregation of duties?

5. Is the Audit Committee aware of any:

    - breaches of, or deficiencies in internal control; and
    - actual, suspected or alleged frauds during 2020/21?

6. Is the Audit Committee aware of any organisational or management pressure to meet financial or operating targets?

7. How does the Audit Committee gain assurance that all relevant laws and regulations have been complied with? Are you aware of any instances of non-compliance during 2020/21?

8. Is the Audit Committee aware of any actual or potential litigation or claims that would affect the financial statements?

9. How does the Audit Committee satisfy itself that it is appropriate to adopt the going concern basis in preparing the financial statements?

10. Has management considered the impact of the coronavirus outbreak as part of their going concern assessment, including:
    - any changes in underlying assumptions
    - additional or potential financial difficulties, impairments or write-offs

11. How does the Audit Committee satisfy itself that the College has arrangements to ensure compliance with the Scottish Funding Council's ("SFC") Accounts Direction and Financial Memorandum?

12. How does the Audit Committee satisfy itself that the College has arrangements to ensure compliance with its requirements as an independent charity as set out by OSCR?

13. How does the Audit Committee satisfy itself that the College has arrangements to monitor and maintain the regularity of income and expenditure?

14. What does the Audit Committee consider to be the related parties that are significant to the College and what is its understanding of the relationships and transactions with those related parties?

15. Does the Audit Committee have concerns regarding relationships or transactions with related parties and, if so, what is the substance of those concerns?

Thank you for your assistance. Please respond to the inquiries above (or if you have any queries in respect of this letter) by emailing Grace Scanlin at Grace.Scanlin@uk.ey.com.

Yours faithfully

Stephen Reid
Partner
For and on behalf of Ernst & Young LLP

Moray College

Annual Audit Plan
Year ending 31 July 2021

Building a better working world

Contents

About this report

This report has been prepared in accordance with Terms of Appointment Letter from Audit Scotland dated 31 May 2016 through which the Auditor General for Scotland has appointed us as external auditor of Moray College ("the College") for financial years 2016/17 to 2020/21. As a result of the impact of Covid-19 our appointment was extended by a further 12 months to include the financial year 2021/22. We undertake our audit in accordance with the Public Finance and Accountability (Scotland) Act 2000 and our responsibilities as set out within Audit Scotland's Code of Audit Practice (the Code), issued on 26 May 2016.

This report is for the benefit of the College and is made available to the Auditor General for Scotland and Audit Scotland (together the Recipients). This report has not been designed to be of benefit to anyone except the Recipients. In preparing this report we have not taken into account the interests, needs or circumstances of anyone apart from the Recipients, even though we may have been aware that others might read this report.

Any party other than the Recipients that obtains access to this report or a copy (under the Freedom of Information Act 2000, the Freedom of Information (Scotland) Act 2002, through a Recipient's Publication Scheme or otherwise) and chooses to rely on this report (or any part of it) does so at its own risk. To the fullest extent permitted by law, Ernst & Young LLP does not assume any responsibility and will not accept any liability in respect of this report to any party other than the Recipients.

Complaints

If at any time you would like to discuss with us how our service to you could be improved, or if you are dissatisfied with the service you are receiving, you may take the issue up with Stephen Reid who is our partner responsible for services under appointment by Audit Scotland, telephone 0131 777 2839, email sreid2@uk.ey.com. If you prefer an alternative route, please contact Hywell Ball, our Managing Partner, 1 More London Place, London SE1 2AF. We undertake to look into any complaint carefully and promptly and to do all we can to explain the position to you. Should you remain dissatisfied with any aspect of our service, or with how your complaint has been handled, you can refer the matter to Diane McGiffen, Audit Scotland, 4th Floor, 102 West Port, Edinburgh, EH3 9DN. Alternatively you may of course take matters up with our professional institute. We can provide further information on how you may contact our professional institute.

1. Executive summary

Our key contacts:

Stephen Reid
Partner
sreid2@uk.ey.com

Grace Scanlin
Senior Manager
Grace.Scanlin@uk.ey.com

Our independence
We confirm that we have undertaken client and engagement continuance procedures, which include our assessment of our continuing independence to act as your external auditor.

Purpose of this report

In accordance with the Public Finance and Accountability (Scotland) Act 2000, Audit Scotland appointed EY as the external auditor of Moray College (the College) for the five year period 2016/17 to 2020/21. As a result of the impact of Covid-19 our appointment was extended by a further 12 months to include the financial year 2021/22.

This Annual Audit Plan, prepared for the benefit of College management and the Audit Committee, sets out our proposed audit approach for the audit of the financial year ending 31 July 2021, the fifth year of our appointment. In preparing this plan, we have updated our understanding of the College through planning discussions with management, review of relevant documentation and committee reports, and our general understanding of the environment in which the College is operating.

A key objective of our audit reporting is to add value by supporting the improvement of the use of public money. We aim to achieve this through sharing our insights from our audit work, our observations around where the College employs best practice and where processes can be improved. We use these insights to form our audit recommendations to support the College in improving its practices around financial management and control, as well as around key aspects of the wider scope dimensions of audit. These are highlighted throughout our reporting together with our judgements and conclusions regarding arrangements.

After consideration by the College's Audit Committee, the plan is provided to Audit Scotland and published on their website.

Scope and Responsibilities

This Annual Audit Plan covers the work that we plan to perform to provide you with our opinion on whether the College's financial statements (the financial statements) give a true and fair view of the College's affairs as at 31 July 2021 in accordance with applicable law and the financial reporting framework. We also report on the regularity of transactions, as required by the Scottish Funding Council.

We undertake our audit in accordance with the Code of Audit Practice ('the Code'), issued by Audit Scotland in May 2016; International Standards on Auditing (UK); relevant legislation; and other guidance issued by Audit Scotland. The Code sets out the responsibilities of both the College and the auditor, more details of which are provided in Appendix A.

Our Financial Statement Audit

We are responsible for conducting an audit of the financial statements of the College. We provide an opinion as to:

- whether they give a true and fair view in accordance with the Further and Higher Education (Scotland) Act 1992 and directions made thereunder by the Scottish Funding Council of the state of the College's affairs as at 31 July 2021 and its surplus or deficit for the year then ended;
- have been properly prepared in accordance with United Kingdom Generally Accepted Accounting Practice, including FRS 102: The Financial Reporting Standard applicable in the UK and Ireland; and
- whether they have been properly prepared in accordance with the Further and Higher Education (Scotland) Act 1992 and directions made thereunder issued by the Scottish Funding Council, the Charities and Trustee Investment (Scotland) Act 2005 and regulation 14 of The Charities Accounts (Scotland) Regulations 2006 (as amended).

We also review and report on the consistency of the other information prepared and published by the College along with the financial statements.

Materiality

Materiality levels have been set at the planning stage of the audit as follows:

Planning Materiality

£304,000

2% of the College's gross forecast expenditure

Tolerable Error

£228,000

Materiality at an individual account level

Nominal amount

£15,000

Level that we will report misstatements to committee

Based on considerations around the expectations of financial statement users and qualitative factors, we apply a lower materiality level to the audited section of the Remuneration Report. We also apply professional judgement to consider the materiality of related party transactions to both parties.

Wider Scope audit

Our responsibilities extend beyond the audit of the financial statements. The Code requires auditors to provide judgements and conclusions on the dimensions of wider scope public audit that are applicable to small bodies:

- Financial sustainability; and
- Governance and transparency.

We will continue to extend our work to consider financial management arrangements at the College in 2021/22.

Our audit work over the wider scope audit dimensions complements our financial statements audit. We have updated our understanding of the risks impacting the College through discussions with management, review of relevant committee reports, and our knowledge of the education sector.

Audit Risk Dashboard

Key Financial Statement Risks

Fraud Risk: Risk of fraud in revenue and expenditure recognition	In accordance with ISA (UK) 240, we consider the presumed fraud risk in respect of improper income recognition. In the public sector, this requirement is modified by Practice Note 10 issued by the Financial Reporting Council, which states that auditors should also consider the risk that material misstatements may occur by the manipulation of expenditure recognition. During 2020/21, we will consider the impact of additional Covid-19 income streams on the College.
Fraud Risk: Misstatement due to fraud or error	As identified in ISA (UK) 240, management is in a unique position to perpetrate fraud due to the ability to manipulate accounting records directly or indirectly and prepare fraudulent financial statements by overriding controls that would otherwise appear to be operating effectively.
Inherent risk: Valuation of property, plant and equipment	The value of property, plant and equipment (PPE) represent significant balances in the College's financial statements. Management is required to make material judgemental inputs, including the assessment of any required impairment, and to apply estimation techniques to calculate the year-end balances recorded in the balance sheet.
Inherent risk: Valuation of pension assets and liabilities	Accounting for the Local Government Pension Scheme (LGPS) involves significant estimation and judgement and therefore management engages an actuary to undertake the calculations on their behalf. The North East Scotland Pension Fund triennial valuation was completed as at 31 March and will therefore inform the valuation as at 31 March 2021. ISAs (UK) 500 and 540 require us to undertake procedures on the use of management experts, the assumptions underlying fair value estimates, and the valuation of the College's share of scheme assets and liabilities at the year end.

Wider Scope Risks

Financial Sustainability: Medium Term Financial Planning	The full impact of the global pandemic on the College's education and financial plans has continued to evolve throughout 2020/21. In the short term, there is the impact of government funding, including furlough income, and direct financial support from the Scottish Funding Council. The College has also managed the move to blended learning well, with relatively few deferrals to 2021/22. As a result, the acute financial pressures facing the College in 2020/21 have eased. The College is due to prepare an updated financial forecast in June 2021. Our expectation is that this will continue to reflect significant financial pressures in the medium to long term. The College's plans to implement a voluntary severance scheme were paused during the pandemic. A previous recovery plan which significantly reduced non-pay expenditure but the impact on the College's infrastructure creates a risk that the College will not be able to develop viable and sustainable financial plans.

2. Sector developments

In accordance with the principles of the Code, our audit work considers key developments in the sector. We obtain an understanding of the strategic environment in which the College operates to inform our audit approach.

The context for financial sustainability in the FE sector

As we noted within our Annual Audit Report, during 2020, the Scottish Funding Council released three reports considering the future of colleges and universities. In October 2020 the Scottish Funding Council (SFC) published their review of coherent provision and sustainability which considered how best the SFC can fulfil its mission of securing coherent provision by post-16 education bodies, and the undertaking of research in these changing times. The review covered future provision, delivery, outcomes and targets, funding models and support for research activity across the college and university sector in Scotland.

Specifically, as part of this review, the SFC published their updated analysis of the sector within their report, The Financial Sustainability of Colleges and Universities in Scotland. This reflects on the specific financial challenges the sector was facing prior to the impact of Covid-19, including cost pressures from cost of living pay awards, employers' pension contributions, maintaining the college estate and the UK's exit from the European Union, and notes that colleges were already implementing transformation plans to address those challenges. Covid-19 has, in some cases, resulted in the delay of these transformation plans, particularly where they relate to severance and commercial income growth. The main impact of Covid-19 is considered to be felt most by the sector during the 2020/21 financial and academic year.

Recognising the financial challenges facing colleges in the upcoming period, the SFC has identified a number of actions to further support colleges including:

- Targets – SFC will not recover funds for shortfalls against outcome agreement targets where these are related to Covid-19;
- Capital Funding – £2.3 million of additional funding for colleges has been awarded to support the provision of ICT equipment to help tackle digital poverty. In addition, the SFC announced £6.5 million of additional capital funding to support the economic recovery in 2020/21;
- Cash advances – SFC has provided flexibility in grant drawdowns to several colleges encountering liquidity challenges; and
- Flexibilities in relation to Flexible Workforce Development Fund, Student Support funds and credits.

We will continue to review the full impact of the financial savings requirements outlined in the Financial Forecast Return (FFR) against the College's strategic objectives as part of our work on financial sustainability.

Additional Funding for Colleges 2020/21

Additional non-recurring Covid-19 support funding was announced as part of the Scottish Government's budget update statement on 16 February 2021. This included an additional £60 million for further and higher education, specifically to support universities and colleges maintain research activity, project jobs, help students and boost research and knowledge exchange.

The SFC subsequently announced additional funding of £15.3 million for colleges on 24 March 2021, applicable for the financial year 2020/21. The SFC noted that this funding will help address the major impact that Covid-19 has had on colleges, including:

- Reduced income, including from commercial contracts and residencies, affecting research funding and putting jobs at risk;
- Additional costs such as adjustments to campuses and facilities to allow for social distancing; and
- General weakening of financial sustainability.

Recognising that all colleges are facing financial pressures, the additional £15.3 million has been allocated to colleges in proportion to their respective core teaching grant allocations for Academic Year 2020/21. The conditions of the grant funding are further outlined within the SFC's *Additional funding for Colleges in FY 2020/21* report, as well as confirmation that the release of this additional funding is to be used for FY 2020/21.

2021/22 Budget

The SFC announced the indicative funding allocations for the Academic Year 2021/22 on 24 March 2021. The indicative funding allocations set out are based on the Scottish Government's draft budget 2021/22 announcement on 28 January 2021 which was approved by the Scottish Parliament on 9 March 2021. The approved Scottish Budget 2021/22 set a College Resource (Revenue) budget for the financial year 2021/22 of £675.7 million, an increase of £35.7 million (5.6%) from 2020/21.

The SFC provides indicative funding allocations to help colleges plan for the forthcoming academic year, with final funding allocations to be published by the end of May 2021. The SFC's indicative funding announcement notes that:

- The SFC's revenue budget for 2021/22 has increased by 10.8% (£70.2 million) from AY 2020/21;
- Teaching funding has been increased by 8% (£29.8 million);
- Student support funding has increased by 1.9% (£2.6 million), and there is additional student support contingency funding set aside;
- The other programme funding budget, which includes national sector-wide services and strategic projects, has increased by £13.1 million;
- Student activity (credit) volume for the sector has been increased by 3.6% (circa 63,000 credits), largely as a result of creditors for Foundation Apprenticeships and deferred students; and
- Capital funding has decreased by £2 million, with sector-wide capital maintenance reducing by 6.2% (£1.8 million).

3. Financial Statement Risks

Introduction

The annual financial statements enables the College to demonstrate accountability for, and its performance in the use of its resources. They are prepared in accordance with proper accounting practice and applicable law.

Audit Opinion

We are responsible for conducting an audit of the financial statements of the College. We will provide an opinion on the financial statements as to:

- whether they give a true and fair view in accordance with the Further and Higher Education (Scotland) Act 1992 and directions made thereunder by the Scottish Funding Council of the state of the College's affairs as at 31 July 2021 and its surplus or deficit for the year then ended;
- have been properly prepared in accordance with United Kingdom Generally Accepted Accounting Practice, including FRS 102: The Financial Reporting Standard applicable in the UK and Ireland; and
- whether they have been properly prepared in accordance with the Further and Higher Education (Scotland) Act 1992 and directions made thereunder issued by the Scottish Funding Council, the Charities and Trustee Investment (Scotland) Act 2005 and regulation 14 of The Charities Accounts (Scotland) Regulations 2006 (as amended).

We also report on the regularity of transactions, as required by the Scottish Funding Council, and review and report on the consistency of the other information prepared and published by the College along with the financial statements.

Other Statutory Information

The management commentary and narrative reporting continues to be an area of increased scrutiny as a result of rising stakeholder expectations, including continuing interest by the Financial Reporting Council. We will therefore continue to work with the finance team to support the continued improvement of the financial statements, including narrative disclosures, in 2020/21.

Audit Approach

We determine which accounts, disclosures and relevant assertions could contain risks of material misstatement. Our audit involves:

- Identifying and assessing the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion.
- Obtaining an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the College's internal control.
- Evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.
- Concluding on the appropriateness of management's use of the going concern basis of accounting.
- Evaluating the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.
- Obtaining sufficient appropriate audit evidence regarding the financial information of the entities or business activities within the College.
- Reading other information contained in the financial statements, including the board's statement that the annual report is fair, balanced and understandable, the Audit Committee reporting appropriately addresses matters communicated by us to the committee and reporting whether it is materially inconsistent with our understanding and the financial statements.
- Maintaining auditor independence.
- Substantive tests of detail of transactions and amounts. For 2020/21 we plan to follow a predominantly substantive approach to the audit as we have concluded this is the most efficient way to obtain the level of audit assurance required to conclude that the financial statements are not materially misstated.

Materiality

For the purposes of determining whether the financial statements are free from material error, in accordance with ISA (UK) 320 we define materiality as the magnitude of an omission or misstatement that, individually or in the aggregate, in light of the surrounding circumstances, could reasonably be expected to influence the economic decisions of the users of the financial statements.

Our evaluation of it requires professional judgement and necessarily takes into account qualitative as well as quantitative considerations implicit in the definition. We would be happy to discuss expectations regarding our detection of misstatements in the financial statements if required.

Materiality Level	Rationale
Planning Materiality £304,000	**Planning materiality (PM)** – the amount over which we anticipate misstatements would influence the economic decisions of a user of the financial statements. For planning purposes, materiality for 2020/21 has been set at £304,000. This represents approximately 2% of the College's forecast expenditure for the year.
Tolerable Error £228,000	**Tolerable error (TE)** – materiality at an individual account balance, which is set so as to reduce to an acceptably low level that the aggregate of uncorrected and undetected misstatements exceeds PM. We have set it at £228,000 which represents 75% of planning materiality.
Summary of Audit Differences £15,000	**Summary of Audit Differences (SAD) Nominal amount** – the amount below which misstatements whether individually or accumulated with other misstatements, would not have a material effect on the financial statements. The Code requires that auditors report at no more than £250,000. We have set it at £15,000, which represents 5% of planning materiality.

In 2019/20, we reduced our materiality due to rapid changes in the external environment in which the College operates. We have determined that in 2021/22 it is appropriate to reinstate materiality at 2%, given the reduced immediate uncertainties in the external environment.

The bases for the materiality outlined are consistent with our approach in previous years. Factors which we consider include the perspectives and expectations of users of the financial statements as well as our risk assessment as to the likelihood of material misstatements arising in the financial statements.

Based on these considerations, we apply lower materiality levels to the following areas we consider to be material by nature rather than size:

- Remuneration Report; and
- Related Party Transactions.

We will therefore review the disclosures related to the above areas in greater detail compared to the materiality thresholds outlined above.

The amount we consider material at the end of the audit may differ from our initial determination. At the end of the audit we will form, and report to you, our final opinion by reference to all matters that could be significant to users of the financial statements, including the total effect of any audit misstatements, and our evaluation of materiality at that date.

Going Concern compliance with ISA 570

We outlined in our 2019/20 reporting to the committee the impact that the Covid-19 pandemic had on the further education sector, and the increased levels of uncertainty within the forecasts used as part of the College's going concern assessment. As a result, in 2019/20, we placed additional focus on significant judgements made to conclude whether events or conditions indicate that a material uncertainty existed that may cast significant doubt on the College's ability to continue as a going concern. The judgements made determined the appropriate disclosures to be made in the financial statements, and allowed us to consider the impact on our audit opinion.

A revised auditing standard relating to our work on going concern, ISA 570, is effective for the audit of the College's 2020/21 financial statements. The revised standard increases the work we have been traditionally required to perform when assessing whether the College is a going concern. It means UK auditors will follow significantly stronger requirements than those required by current international standards, and much more in line with the required work undertaken by management and the audit team in 2019/20.

Auditing standards have been revised in response to enforcement cases and well-publicised corporate failures where the auditor's report failed to highlight concerns about the prospects of entities which collapsed shortly afterwards.

The revised standard requires:

- challenge of management's identification of events or conditions impacting going concern, more specific requirements to test management's resulting assessment of going concern, an evaluation of the supporting evidence obtained which includes consideration of the risk of management bias;
- greater work for us to challenge management's assessment of going concern, thoroughly test the adequacy of the supporting evidence we obtained and evaluate the risk of management bias. Our challenge will be made based on our knowledge of the College obtained through our audit, which will include additional specific risk assessment considerations which go beyond the current requirements;
- improved transparency with a new reporting requirement for public interest entities, listed and large private companies to provide a clear, positive conclusion on whether management's assessment is appropriate, and to set out the work we have done in this respect. While the College is not one of these three entity types listed, we will ensure compliance with any updated reporting requirements;
- a stand back requirement to consider all of the evidence obtained, whether corroborative or contradictory, when we draw our conclusions on going concern; and
- necessary consideration regarding the appropriateness of financial statement disclosures around going concern.

A revised version of Practice Note 10 Audit of Financial Statements and Regularity of Public Sector Bodies in the UK (PN 10) was issued in November 2020. A significant aspect of PN 10 is the guidance on applying ISA (UK) 570 Going Concern to the public sector. This notes the importance of the applicable financial reporting framework in determining the extent of the auditor's procedures. Our work will also take cognisance of recent guidance issued by Audit Scotland. As in prior years, due to the anticipated continuation of service provision, the going concern basis of accounting will continue to be appropriate for the College.

Covid-19 - Impact on Financial Statements

In our reporting through 2020, we outlined how the ongoing disruption to daily life and the economy as a result of the Covid-19 virus was having a pervasive impact upon the preparation of financial statements for all bodies across the further education sector, and will do so for the foreseeable future. Financial statements now need to reflect the impact of Covid-19 on the College's financial position and performance. There continues to be a wide range of ways in which Covid-19 can impact the financial statements, potentially impacting the accounting and disclosure requirements throughout. We have outlined through this report how these may include, at a minimum:

- Management's assessment of going concern.
- Revenue recognition accounting for where activity has materially changed and where new income streams have occurred such as from government support.
- The valuation of fixed assets, in particular the ongoing use of the College estate.
- The valuation of future pension liabilities and scheme assets.
- Potential impairment of receivables.
- Financial statement disclosures, including the Annual Governance Statement.

We will report on the full impact of Covid-19 on the College's financial statements, and how we have responded to the additional risks of misstatement, as part of our reporting at the yearend to the committee, including supplementing this audit planning report with any material changes to our detailed risk assessment and audit approach for the yearend audit, where required.

Covid-19 – Impact on Audit Process

The extensive nature of the Covid-19's impact on the financial statements and underlying accounting arrangements drives our assessment that the risk is considered pervasive to the financial statement audit. In addition to the impact on the financial statements themselves, the disruption caused by Covid-19 may impact on management's ability to produce financial statements and our ability to complete the audit to the planned timetable. For example, it will continue to be more difficult than usual for finance teams to collate and for us to access the supporting documentation necessary to support our audit procedures. As with the 2019/20 audit, this will need to be mitigated by additional audit procedures to respond to the additional risks caused by the factors noted above.

We have outlined the planned timing for the key deliverables of the audit process in Appendix D. These reflect the agreed intention to continue to work closely with management to review timeframes and logistics for the completion of the audit in 2020/21. All deadlines will continue to be reviewed throughout the year as circumstances change, however the FRC and Audit Scotland have made clear that any deadlines are secondary to the primacy of audit quality and ensuring completeness of work regardless of the environment in which audit takes place.

We will aim to take a pragmatic and flexible approach in the current environment.

Significant Risks

We have set out the significant risks (including fraud risks) identified for the current year audit along with the rationale and expected audit approach. The risks identified may change to reflect any significant findings or subsequent issues we identify during the audit.

Significant Risk - Risk of fraud in income and expenditure recognition

Under ISA 240 there is a presumed risk that income may be misstated due to improper recognition of revenue. In the public sector, this requirement is modified by Practice Note 10, issued by the Financial Reporting Council, which means we also consider the risk that material misstatements may occur by the manipulation of expenditure recognition.

Other than income and expenditure recognition, we have not identified any specific areas where management override will manifest as a significant fraud risk, however we will continue to consider this across the financial statements throughout the audit.

We consider there to be a specific risk around SFC income and expenditure recognition through: ▸ Incorrect income and expenditure cut-off recognition to alter the College's financial position around the financial year end. ▸ Incorrect recognition applied to grant income with conditions. We also recognise a revenue recognition risk for other SFC grants where performance conditions are in place, tuition fee income and other grants and operating income in respect of possible manipulation of cut-off around the financial year end. We recognise the same risk around incorrect recognition of other operating expenditure in line with Practice Note 10.	Work we will undertake: ▸ review and test all relevant income and expenditure policies against the relevant accounting standards and SORP ▸ review, test and challenge management around any accounting estimates on income and expenditure recognition for evidence of bias ▸ develop a testing strategy to test all material income and expenditure streams ▸ test all material grant income with performance conditions to ensure the income is recognised correctly in line with the outlined requirements ▸ review and perform focused testing on income and expenditure around the year end to ensure correct recognition around cut-off between financial periods ▸ perform testing for any evidence of clawback of income where conditions for entitlement have not been met ▸ review and develop a testing strategy for Covid-19 related income streams, including furlough income and additional Covid-19 related grant income ▸ assess and challenge manual adjustments or journal entries by management around the year end for evidence of management bias and evaluation of business rationale and evidence

Fraud Risk – Misstatement due to fraud or error

Management has the primary responsibility to prevent and detect fraud. It is important that management, with the oversight of those charged with governance, has put in place a culture of ethical behaviour and a strong control environment that both deters and prevents fraud.

The risk of management override is pervasive to the audit and impacts the testing of all areas. Our responsibility is to plan and perform audits to obtain reasonable assurance about whether the financial statements as a whole are free of material misstatements whether caused by error or fraud. As auditor, we approach each engagement with a questioning mind that accepts the possibility that a material misstatement due to fraud could occur, and design the appropriate procedures to consider such risk. This takes account of the fact that management are in a unique position to override controls which otherwise appear to be operating effectively.	Based on the requirements of auditing standards our approach will focus on: ▸ identifying fraud risks during the planning stages ▸ inquiry of management about risks of fraud and the controls put in place to address those risks including segregation of duties ▸ consideration of the effectiveness of management's controls designed to address the risk of fraud ▸ determining an appropriate strategy to address those identified risks of fraud ▸ performing mandatory procedures regardless of specifically identified fraud risks, including testing of journal entries and other adjustments in the preparation of the financial statements ▸ specific focus on the accounting for any identified key areas of judgement and estimates in the financial statements and significant and unusual transactions. This will include consideration of any provisions requiring to be made as at the balance sheet date for any restructuring arrangements entered into by the College, as applicable. From 2020/21, our work around estimates in particular will be required to comply with the requirements around the revised ISA (UK) 540.

We will report our findings in these areas to you within our 2020/21 Annual Audit Report.

Inherent Risk – Valuation of Property, Plant & Equipment

The College's property portfolio totals £25.6 million as at 31 July 2020 (*2018/19 £25.4 million*), with the major elements of this being in respect of land and buildings. Land and buildings are revalued to fair value with a full revaluation taking place at least every five years.

The valuation of property, plant and equipment is assessed as an inherent risk. Management involves specialists in the preparation of these accounting valuations. We utilise our own specialists, as appropriate, to support the core audit team in the performance of audit procedures on these balances.	The College is required to consider annually that the valuation of the College estate remains appropriate outside of formal revaluation cycles. Management engaged external valuers to conduct a full valuation of the land and buildings estate as at 31 July 2019. Given the size of this balance and the number of assumptions that are made in the valuation, we assign a higher inherent risk to property, plant and equipment. The impact of Covid-19 on the use of assets and future plans means that we will place significant scrutiny on management's assessment of impairment.	Our approach will focus on: ▸ analysis of the source data and inquiries as to the procedures used by management's specialist to establish whether the source data is complete ▸ assessment of the reasonableness of the assumptions and methods used, including their compliance with the SORP ▸ consideration of the appropriateness of the timing of when the specialist carried out the work ▸ assessment of whether the substance of the specialist's findings are properly reflected in the financial statements ▸ consideration of the material uncertainty that management's specialist may add to their valuation reports due to Covid-19, and the potential impact on our audit approach and opinion. We may consult as required. ▸ assessment of the potential for impairment across the College estate that has not been reflected in the financial statements or most recent formal valuation ▸ assessment of specialist's findings for assets held for resale, and whether these valuations have been correctly processed in the financial statements through testing of accounting entries ▸ assessment of the College's backlog maintenance estates plans, including consideration of whether backlog maintenance expenditure in the year has been correctly accounted for as capital or revenue expenditure.

Inherent Risk – Valuation of Pension Liabilities

The College participates in two pension schemes: the North East Scotland Pension Fund (NESPF), and the Scottish Teachers Superannuation Scheme (STSS). While both are defined benefit pension schemes, the College is unable to identify its share of the underlying assets and liabilities of the STSS scheme on a consistent and reasonable basis and therefore, the scheme is accounted for as if it were a defined contribution scheme.

The Further and Higher Education SORP and the SFC Accounts Direction require the College to make extensive disclosures within the financial statements regarding its membership of the North East Scotland Pension Fund.

The information disclosed is based on the report issued by the College's actuary.

Triennial valuations of Scottish Local Government Pension Schemes (LGPS) were completed in March 2021. This will identify the funding level in each scheme and inform future funding and investment strategies as well as determining the level of employer and employee contribution rates from 2021/22 onwards.

NESPF is accounted for as a defined benefit scheme. The net pension liabilities on the balance sheet arising from participation in the scheme at 31 July 2020 were £29.5 million (*2018/19: £25.9 million).*

Accounting for this scheme involves significant estimation and judgement, including financial and demographic assumptions. The College engages an actuary to undertake the calculations on their behalf.

ISAs (UK) 500 and 540 require us to undertake procedures on the use of management experts and the assumptions underlying fair value estimates.

Our approach will include:

- obtaining an actuarial report at the year end date for the scheme and considering the reasonableness and consistency of assumptions underpinning such reports, in light of guidance available
- performing substantive testing on the verification of the pension assets, by engaging with the auditor of North East Scotland Pension Fund in line with the assurance protocols laid out by Audit Scotland for IAS 19
- engage our actuarial specialists to assess the work of the actuary (Mercer), including the assumptions they have used and their assessment of the liability due to recent legal rulings including McCloud and Goodwin
- we will also review the calculation of the College's valuation of future early retirement liabilities at 31 July 2021
- review and test the accounting entries and disclosures made within the College's financial statements in relation to IAS 19.

Other audit considerations

We also plan and perform certain general audit procedures on every audit which may not be directly related to financial statement account assertions. Examples of such procedures includes compliance with applicable laws and regulations, litigation and claims and related parties.

Accounting Framework: Updated SFC Accounts Direction

The SFC's Accounts Direction is published annually in July and provides College's with guidance on disclosure requirements for the financial statements. We will work with management during 2020/21 to ensure the correct application of new requirements.

Changes to Auditing Standards

A revised ISA (UK) 701 applies from 2020/21 and aims to secure enhancements to auditor reporting. Our Annual Audit Report will therefore include:

- a description of the most significant assessed risks of material misstatement that were identified by the auditor which had the greatest effect on the overall audit strategy, the allocation of resources in the audit, and directing the efforts of the audit team;
- how each of the above significant risks of material misstatement was addressed including, as a new requirement of the ISA, significant judgements made with respect to each one;
- specifying the materiality threshold for the financial statements as a whole and, as new requirements, specifying performance materiality and providing an explanation of the significant judgments in determining these amounts; and
- an overview of the scope of the audit, including an explanation of how it addressed each of the significant assessed risks of material misstatement and how it was influenced by the auditor's application of materiality.

ISA(UK) 540 on accounting estimated was issues in December 2019. Guidance on inherent risk factors relevant to the public sector includes examples to be considered such as:

- a very high degree of estimation uncertainty caused by the need to project forecasts far into the future, such as liabilities relating to defined benefit pension schemes
- areas where there may be a lack of available comparators for estimates that are unique to the public sector, such as the valuation of important public assets
- the existence of possible constructive obligations created by political statements or past practice of carrying out actions that may be expected of public authorities but are not required by law; and
- political uncertainty and the possibility of future changes in public policy having an impact on the assumptions used to prepare accounting estimates.

Use of specialists

When auditing key judgements, such as the valuation of property, plant and equipment, defined benefit pension scheme assets and liabilities, or certain assets and liabilities, we are often required to rely on the input and advice provided by specialists who have qualifications and expertise not possessed by the core audit team. In accordance with Auditing Standards, we will evaluate each specialist's professional competence and objectivity, considering their qualifications, experience and available resources, together with the independence of the individuals performing the work.

We also consider the work performed by the specialist in light of our knowledge of the College's business and processes and our assessment of audit risk in the particular area. For example, we would typically perform the following procedures:

- Analyse source data and make inquiries as to the procedures used by the specialist to establish whether the source data is relevant and reliable.
- Assess the reasonableness of the assumptions and methods used.
- Consider the appropriateness of the timing of when the specialist carried out the work.
- Assess whether the substance of the specialist's findings are properly reflected in the financial statements.

Internal audit

We will review the internal audit plan and the results of internal audit's work, including the discussion of audit findings at the Audit Committee and management's response to findings. We will reflect the findings from internal audit reports, together with reports from any other work completed in the year, in our plan for the audit, where they raise issues that could have an impact on the financial statements or our wider responsibilities.

Cyber Security

As outlined by Audit Scotland within their report *Fraud and Irregularity Update 2019/20*, the Covid-19 pandemic has brought significant challenges across the public sector as bodies have sought to continue to deliver services during extremely difficult times. In such emergency situations, existing controls may be compromised and it can be difficult to put in place robust controls for new processes.

The report highlights that there has been an increase in cybercrime, as more public sector staff connect remotely, including the use of various online video conferencing services for meetings which pose security issues. The report also highlights an increase in phishing emails and scams which, if accessed, allow fraudulent access to public sector systems.

We will discuss with management their assessment of whether internal controls at the College are sufficiently robust to mitigate the risk of cyber attacks.

Other audit responsibilities

Under the terms of our appointment, our role and responsibilities include a number of other assurance activities. This includes the provision of information to support Audit Scotland national reports and studies.

Anti-money laundering

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 came into force on 26 June 2017 and replace The Money Laundering Regulations 2007. The regulations impose an obligation on the Auditor General to inform the National Crime Agency if he knows or suspects that any person has engaged in money laundering or terrorist financing. As appointed auditor we will consider arrangements for the College to identify and report any instances of money laundering in line with Audit Scotland reporting arrangements.

Data analytics

Where possible and appropriate, we will use our bespoke data analysers to enable us to capture whole populations of your financial data, in particular covering journal entries and payroll transactions. These analysers help identify specific exceptions and anomalies within populations of data to focus substantive audit tests more effectively than traditional audit sampling.

We will report the findings of our work, including any significant weaknesses or inefficiencies identified and recommendations for improvement, to management and the Audit Committee through the yearend audit reporting process.

4. Wider Scope Dimensions: Risk assessment and approach

Covid-19 is a pervasive risk that impacts all wider scope dimensions. This will be an area of audit focus for 2020/21 considering how the College has adapted and the implications for the College's finances.

Together the Accounts Commission and the Auditor General for Scotland agreed the two dimensions set out in the Code which comprise the wider scope audit for small public sector bodies in Scotland. These are:

- Financial Sustainability; and
- Governance and Transparency.

We will continue to extend our work to consider financial management arrangements at the College in 2021/22.

Basis for risk assessment

The Code sets out an expectation that 'significant' risks identified through our planning process that relate to the wider scope dimensions will be communicated with you.

As part of our risk assessment procedures, we have reviewed each dimension to assess potential areas of risk. We set out our areas of focus, along with any specific significant risks relating to each dimension below.

Financial Management

As in 2019/20, we will continue to assess the impact of Covid-19 and the subsequent lockdowns on any core financial management arrangements. We will therefore consider:

- How internal control arrangements are being adapted and monitored to respond to ongoing remote working arrangements;
- How the College continue to respond to budgetary pressures including the loss of non-SFC income; and
- Whether financial reporting to the Board and Finance and Resources Committee continued and whether there was a clear articulation of the financial risks.

Financial Sustainability

Financial sustainability considers the medium and longer term outlook for the College to determine if planning is effective to support service delivery. We focus on the arrangements to develop viable and sustainable financial plans.

In 2019/20, the College prepared a three-year financial forecast for the period 2020 to 2023 and submitted these to the SFC in the form of the template Financial Forecast Return ('FFR'). The forecast is based on assumptions provided by the SFC in addition to College specific assumptions for areas such as other income and staff numbers, as included within the College's Budget 2020/21 and Financial Plan 2021/22 to 2022/23.

Medium term financial planning

The full impact of the global pandemic on the College's education and financial plans has continued to evolve throughout 2020/21. In the short term, there is the impact of government funding, including furlough income, and direct financial support from the Scottish Funding Council. The College has also managed the move to blended learning well, with relatively few deferrals to 2021/22. As a result, the acute financial pressures facing the College in 2020/21 have eased.

The College is due to prepare an updated financial forecast in June 2021. Our expectation is that this will continue reflect significant financial pressures in the medium to long term. The College's plans to implement a voluntary severance scheme were paused during the pandemic. A previous recovery plan which significantly reduced non-pay expenditure but the impact on the College's infrastructure creates a risk that the College will not be able to develop viable and sustainable financial plans.

Our work for the year will consider:

- Has the College revised medium term financial plans to take account of the materialising risks in relation to Covid-19 and has appropriate scenario planning taken place?
- The impact of wider work undertaken by the Regional Strategic Body to secure financial sustainability across the partnership; and
- Where gaps in financial plans are identified, the approach adopted by the College to engage with the Scottish Funding Council and other stakeholders to address these gaps.

Governance and Transparency

We will continue to consider how governance arrangements were adapted during the Covid-19 pandemic to ensure good governance arrangements remained in place.

Governance and transparency is concerned with the effectiveness of scrutiny and governance arrangements, leadership and decision making, and transparent reporting of financial and performance information.

In our 2019/20 Annual Audit Report we concluded that the College had in place the key requirements for good governance, and concluded that these key features of good governance remained in place and were operating effectively throughout the Covid-19 lockdown. We concluded that the Annual Governance Statement materially complied with the SFC's 2019/20 Accounts Direction.

The College's Audit Committee has an independent chair. Standing Orders regulate how the business of the College is conducted, and detailed terms of reference are in place for the Board's standing committees. The College continues to embed its risk management arrangements, including updating and reporting on the Strategic Risk Register to the Audit Committee.

Our work for the year will consider:

- How the College ensured the quality of arrangements to support good governance during the Covid-19 pandemic, including ensuring that there is sufficient transparency around governance and decision making arrangements?
- Is the Annual Governance Statement within the financial statements complete and does it reflect key matters impacted by Covid-19, such as delays in the completion of internal audit work and non-compliance with the code of good governance where actions were not able to be implemented?
- Progress against prior year audit recommendations from both internal and external audit, including the College's arrangements for ensuring these are monitored and reported on a routine basis.
- Internal audit arrangements during 2020/21, including whether the internal audit programme was able to be completed.

In line with auditing standards, as part of our consideration of the College's governance arrangements, we will be writing to the College Audit Committee to confirm how those charge with governance ensure oversight of management and appropriate governance arrangements are in place. This is not reflective of specific risks identified at the College, but rather in line with our process to annually make formal inquiries beyond standard management meetings and representations.

Appendices

A – Code of Audit Practice: responsibilities

B – Independence and audit quality

C – Required communications with the Audit Committee

D – Timing and deliverables of the audit

E – Audit fees

F – Additional audit information

Appendix A: Code of Audit Practice Responsibilities

Audited Body's Responsibilities

Corporate Governance	Each body, through its chief executive or accountable officer, is responsible for establishing arrangements to ensure the proper conduct of its affairs including the legality of activities and transactions, and for monitoring the adequacy and effectiveness of these arrangements. Audited bodies should involve those charged with governance (including Audit Committees or equivalent) in monitoring these arrangements.
Financial Statements and related reports	Audited bodies must prepare an annual report and accounts containing financial statements and other related reports. They have responsibility for: ▸ preparing financial statements which give a true and fair view of their financial position and their expenditure and income, in accordance with the applicable financial reporting framework and relevant legislation. ▸ maintaining accounting records and working papers that have been prepared to an acceptable professional standard and support their financial statements and related reports disclosures. ▸ ensuring the regularity of transactions, by putting in place systems of internal control to ensure that they are in accordance with the appropriate authority. ▸ maintaining proper accounting records. ▸ preparing and publishing, along with their financial statements, an annual governance statement, management commentary (or equivalent) and a remuneration report that are consistent with the disclosures made in the financial statements. Management commentary should be fair, balanced and understandable and also clearly address the longer-term financial sustainability of the body. ▸ Management, with the oversight of those charged with governance, should communicate clearly and concisely relevant information to users about the entity and its financial performance, including providing adequate disclosures in accordance with the applicable financial reporting framework. Audited bodies are responsible for developing and implementing effective systems of internal control as well as financial, operational and compliance controls. These systems should support the achievement of their objectives and safeguard and secure value for money from the public funds at their disposal. They are also responsible for establishing effective and appropriate internal audit and risk-management functions.
Standards of conduct / prevention and detection of fraud and error	Audited bodies are responsible for establishing arrangements for the prevention and detection of fraud, error and irregularities, bribery and corruption and also to ensure that their affairs are managed in accordance with proper standards of conduct by putting proper arrangements in place.
Financial Position	Audited bodies are responsible for putting in place proper arrangements to ensure that their financial position is soundly based having regard to: ▸ such financial monitoring and reporting arrangements as may be specified ▸ compliance with any statutory financial requirements and achievement of financial targets ▸ balances and reserves, including strategies about levels and their future use ▸ how they plan to deal with uncertainty in the medium and longer term ▸ the impact of planned future policies and foreseeable developments on their financial position.
Best Value	The Scottish Public Finance Manual sets out that accountable officers appointed by the Principal Accountable Officer for the Scottish Administration have a specific responsibility to ensure that arrangements have been made to secure best value.

Appendix B: Independence Report

The FRC Ethical Standard and ISA (UK) 260 "Communication of audit matters with those charged with governance", requires us to communicate with you on a timely basis on all significant facts and matters that bear upon our integrity, objectivity and independence. The Ethical Standard, as revised in June 2016, requires that we communicate formally both at the planning stage and at the conclusion of the audit, as well as during the course of the audit if appropriate. The aim of these communications is to ensure full and fair disclosure by us to those charged with your governance on matters in which you have an interest.

Required communications	
Planning stage	Final stage
► The principal threats, if any, to objectivity and independence identified by Ernst & Young (EY) including consideration of all relationships between you, your affiliates and directors and us; ► The safeguards adopted and the reasons why they are considered to be effective, including any Engagement Quality review; ► The overall assessment of threats and safeguards; ► Information about the general policies and process within EY to maintain objectivity and independence. ► Where EY has determined it is appropriate to apply more restrictive independence rules than permitted under the Ethical Standard	► In order for you to assess the integrity, objectivity and independence of the firm and each covered person, we are required to provide a written disclosure of relationships (including the provision of non-audit services) that may bear on our integrity, objectivity and independence. This is required to have regard to relationships with the entity, its directors and senior management, its affiliates, and its connected parties and the threats to integrity or objectivity, including those that could compromise independence that these create. We are also required to disclose any safeguards that we have put in place and why they address such threats, together with any other information necessary to enable our objectivity and independence to be assessed; ► Details of non-audit services provided and the fees charged in relation thereto; ► Written confirmation that the firm and each covered person is independent and, if applicable, that any non-EY firms used in the group audit or external experts used have confirmed their independence to us; ► Written confirmation that all covered persons are independent; ► Details of any inconsistencies between FRC Ethical Standard and your policy for the supply of non-audit services by EY and any apparent breach of that policy; ► Details of any contingent fee arrangements for non-audit services provided by us or our network firms; and ► An opportunity to discuss auditor independence issues

In addition, during the course of the audit, we are required to communicate with you whenever any significant judgements are made about threats to objectivity and independence and the appropriateness of safeguards put in place, for example, when accepting an engagement to provide non-audit services.

We also provide information on any contingent fee arrangements, the amounts of any future services that have been contracted, and details of any written proposal to provide non-audit services that has been submitted;

We ensure that the total amount of fees that EY and our network firms have charged to you and your affiliates for the provision of services during the reporting period, analysed in appropriate categories, are disclosed.

We confirm that we have undertaken client and engagement continuance procedures, which include our assessment of our continuing independence to act as your external auditor.

Relationships, services and related threats and safeguards

We highlight the following significant facts and matters that may be reasonably considered to bear upon our objectivity and independence, including the principal threats, if any. We have adopted the safeguards noted below to mitigate these threats along with the reasons why they are considered to be effective. However we will only perform non-audit services if the service has been pre-approved in accordance with your policy.

Overall Assessment	Overall, we consider that the safeguards that have been adopted appropriately mitigate the principal threats identified and we therefore confirm that EY is independent and the objectivity and independence of Stephen Reid, your audit engagement partner, and the audit engagement team have not been compromised.
Self interest threats	A self interest threat arises when EY has financial or other interests in the Group. Examples include where we have an investment in your company; where we receives significant fees in respect of non-audit services; where we need to recover long outstanding fees; or where we enter into a business relationship with you. At the time of writing, there are no long outstanding fees. We believe that it is appropriate for us to undertake permissible non-audit services and we will comply with the policies that you have approved. None of the services are prohibited under the FRC's Ethical Standard and the services have been approved in accordance with your policy on pre-approval. In addition, when the ratio of non-audit fees to audit fees exceeds 1:1, we are required to discuss this with our Ethics Partner, as set out by the FRC Ethical Standard, and if necessary agree additional safeguards or not accept the non-audit engagement. At the time of writing, the current ratio of non-audit fees to audit fees is approximately 0% (Appendix E), and will continue to be monitored through the audit engagement. No additional safeguards are required. A self interest threat may also arise if members of our audit engagement team have objectives or are rewarded in relation to sales of non-audit services to you. We confirm that no member of our audit engagement team, including those from other service lines, has objectives or is rewarded in relation to sales to you. There are no other self interest threats at the date of this report.
Self review threats	Self review threats arise when the results of a non-audit service performed by EY or others within the EY network are reflected in the amounts included or disclosed in the financial statements. There are no self review threats at the date of this report.
Management threats	Partners and employees of EY are prohibited from taking decisions on behalf of management of the Group. Management threats may also arise during the provision of a non-audit service in relation to which management is required to make judgements or decision based on that work. There are no management threats at the date of this report.
Other threats	Other threats, such as advocacy, familiarity or intimidation, may arise. There are no other threats at the date of this report.

New UK Independence Standards

The Financial Reporting Council (FRC) published the Revised Ethical Standard 2019 in December and it will apply to accounting periods starting on or after 15 March 2020. A key change in the new Ethical Standard will be a general prohibition on the provision of non-audit services by the auditor (and its network) which will apply to UK Public Interest Entities (PIEs). A narrow list of permitted services will continue to be allowed.

Summary of key changes	Overall, we consider that the safeguards that have been adopted appropriately mitigate the principal threats identified and we therefore confirm that EY is independent and the objectivity and independence of Stephen Reid, your audit engagement partner, and the audit engagement team have not been compromised.
	▸ Extraterritorial application of the FRC Ethical Standard to UK PIE and its worldwide affiliates;
	▸ A general prohibition on the provision of non-audit services by the auditor (or its network) to a UK PIE, its UK parent and worldwide subsidiaries;
	▸ A narrow list of permitted services where closely related to the audit and/or required by law or regulation;
	▸ Absolute prohibition on the following relationships applicable to UK PIE and its affiliates, including material significant investees/investors:
	  ▸ Tax advocacy services
	  ▸ Remuneration advisory services
	  ▸ Internal audit services
	  ▸ Secondment/loan staff arrangements
	▸ An absolute prohibition on contingent fees;
	▸ Requirement to meet the higher standard for business relationships i.e. business relationships between the audit firm and the audit client will only be permitted if it is inconsequential;
	▸ Permitted services required by law or regulation will not be subject to the 70% fee cap;
	▸ Grandfathering will apply for otherwise prohibited non-audit services that are open at 15 March 2020 such that the engagement may continue until completed in accordance with the original engagement terms;
	▸ A requirement for the auditor to notify the Audit Committee where the audit fee might compromise perceived independence and the appropriate safeguards;
	▸ A requirement to report to the audit committee details of any breaches of the Ethical Standard and any actions taken by the firm to address any threats to independence. A requirement for non-network component firm whose work is used in the group audit engagement to comply with the same independence standard as the group auditor. Our current understanding is that the requirement to follow UK independence rules is limited to the component firm issuing the audit report and not to its network. This is subject to clarification with the FRC.

Next steps	We will continue to monitor and assess all ongoing and proposed non-audit services and relationships to ensure they are permitted under FRC Revised Ethical Standard 2019 which has been effective from 1 August 2020. At the time of writing this report (May 2021) we do not currently provide any non-audit services which would be prohibited under the new standard.

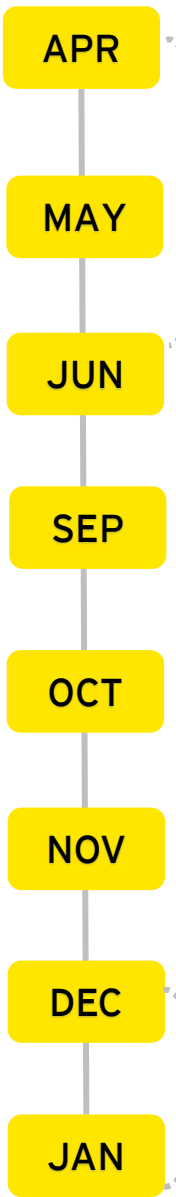
Appendix C: Required Communications

Required communication	Our reporting to you
Terms of engagement / Our responsibilities Confirmation by the Audit Committee of acceptance of terms of engagement as written in the engagement letter signed by both parties. Our responsibilities are as set out in our engagement letter.	Audit Scotland Terms of Appointment letter – audit to be undertaken in accordance with the Code of Audit Practice
Planning and audit approach Communication of the planned scope and timing of the audit, any limitations and the significant risks identified.	Annual Audit Plan
Significant findings from the audit ▸ Our view about the significant qualitative aspects of accounting practices including accounting policies, accounting estimates and financial statement disclosures ▸ Significant difficulties, if any, encountered during the audit ▸ Significant matters, if any, arising from the audit that were discussed with management ▸ Written representations that we are seeking ▸ Expected modifications to the audit report ▸ Other matters if any, significant to the oversight of the financial reporting process	Annual Audit Plan Annual Audit Report
Going concern Events or conditions identified that may cast significant doubt on the entity's ability to continue as a going concern, including: ▸ Whether the events or conditions constitute a material uncertainty ▸ Whether the use of the going concern assumption is appropriate in the preparation and presentation of the financial statements ▸ The adequacy of related disclosures in the financial statements	Annual Audit Report
Misstatements ▸ Uncorrected misstatements and their effect on our audit opinion, unless prohibited by law or regulation ▸ The effect of uncorrected misstatements related to prior periods ▸ A request that any uncorrected misstatement be corrected ▸ Corrected misstatements that are significant ▸ Material misstatements corrected by management	Annual Audit Report
Fraud ▸ Enquiries of the Audit Committee to determine whether they have knowledge of any actual, suspected or alleged fraud affecting the entity ▸ Any fraud that we have identified or information we have obtained that indicates that a fraud may exist ▸ Unless all of those charged with governance are involved in managing the entity, any identified or suspected fraud involving: a. Management; b. Employees who have significant roles in internal control; or c. Others where the fraud results in a material misstatement in the financial statements ▸ The nature, timing and extent of audit procedures necessary to complete the audit when fraud involving management is suspected ▸ Any other matters related to fraud, relevant to Audit Committee responsibility	Annual Audit Report

Required communication	Our reporting to you
Related parties Significant matters arising during the audit in connection with the entity's related parties including, when applicable: ▸ Non-disclosure by management ▸ Inappropriate authorisation and approval of transactions ▸ Disagreement over disclosures ▸ Non-compliance with laws and regulations ▸ Difficulty in identifying the party that ultimately controls the entity	Annual Audit Report or as occurring if material.
Consideration of laws and regulations ▸ Audit findings regarding non-compliance where the non-compliance is material and believed to be intentional. This communication is subject to compliance with legislation on tipping off ▸ Enquiry of the Audit Committee into possible instances of non-compliance with laws and regulations that may have a material effect on the financial statements and that the Audit Committee may be aware of	Annual Audit Report or as occurring if material.
Independence Communication of all significant facts and matters that bear on EY's, and all individuals involved in the audit, objectivity and independence Communication of key elements of the audit engagement partner's consideration of independence and objectivity such as: ▸ The principal threats ▸ Safeguards adopted and their effectiveness ▸ An overall assessment of threats and safeguards ▸ Information about the general policies and process within the firm to maintain objectivity and independence Communication whenever significant judgements are made about threats to objectivity and independence and the appropriateness of safeguards put in place.	Annual Audit Plan Annual Audit Report
Internal controls Significant deficiencies in internal controls identified during the audit	Annual Audit Report
Representations We will request written representations from management and/or those charged with governance.	Annual Audit Report
Subsequent events Where appropriate, asking the Audit Committee whether any subsequent events have occurred that might affect the financial statements.	Annual Audit Report
Material inconsistencies and misstatements Material inconsistencies or misstatements of fact identified in other information which management has refused to revise	Annual Audit Report
Fee Reporting ▸ Breakdown of fee information when the audit plan is agreed ▸ Breakdown of fee information at the completion of the audit ▸ Any non-audit work	Annual Audit Plan Annual Audit Report

Appendix D: Timing and deliverables of the audit

We deliver our audit in accordance with guidance from Audit Scotland. We would note that we continue to operate in a Covid environment and therefore continue to experience delays in audit processes. The delivery of deadlines will be reviewed through the year as circumstances change, however the FRC has made clear that any deadlines are secondary to the primacy of audit quality and ensuring completeness of work regardless of the environment in which audit takes place. We will work with management and the committee secretariat to agree a timetable for the completion of the audit that ensures a smooth governance process.



Audit Activity	Deliverable	Timing
▸ Audit planning and setting scope and strategy for the 2020/21 audit	Annual Audit Plan	May 2021
▸ Walkthrough Visit	Completion of internal documentation	June 2021
▸ Review of current issues impacting the College	Quarterly current issue return submission	Quarterly
▸ Review of reported frauds	Quarterly fraud return submission	Quarterly
▸ Year-end substantive audit fieldwork on unaudited financial statements	Audited Financial Statements	TBC
▸ Conclude on results of audit procedures	Issue Annual Audit Report	TBC
▸ Issue opinion on the College's financial statements	Submit Audit Scotland minimum dataset request	TBC

Appendix E: Audit fees

The audit fee is determined in line with Audit Scotland's fee setting arrangements, set out in recent communications to all audited bodies in line with their publication on '*Our Approach to setting audit fees*' (http://www.audit-scotland.gov.uk/uploads/docs/um/audit_fee_approach.pdf).

Audit Fees	2020/21	2019/20
Component of fee:		
Auditor remuneration – expected fee	**£16,610**	**£16,130**
Additional audit procedures (see below)	**£TBD**	**£6,400**
Audit Scotland fixed charges:		
Pooled costs	**£1,070**	**£920**
Contribution to Audit Scotland costs	**£700**	**£880**
Total fee	**£TBD**	**£24,330**

The expected fee for each body, which for 2020/21 has been set centrally by Audit Scotland, assumes that it has sound governance arrangements in place and operating effectively throughout the year, prepares comprehensive and accurate draft financial statements and supporting schedules, and meets the agreed timetable for the audit. It also assumes there is no major change in respect of the scope of work in the year and an unqualified audit opinion resulting from the audit.

Should any of these circumstances not be in place throughout the audit, it is expected that additional costs will be incurred through the course of the audit which will be subject to recovery in line with the agreed process and rates set out by Audit Scotland. Under this process, fees can be agreed between the auditor and audited body by varying the auditor remuneration by up to 10% above the level set, or more with the approval of Audit Scotland.

We will continue to consider the impact of Covid-19 on the audit throughout 2020/21. At this stage, we estimate that the additional work required to reflect the going concern considerations outlined on page 11 will incur additional fees. Should any additional audit requirements arise we will raise these with management through the course of the audit and agree variations as appropriate, and report the final position to the Audit Committee with our annual audit report.

All fee variations will depend on the progress made by management in providing robust impact assessments and supporting schedules in line with the underlying accounting requirements outlined by the Scottish Funding Council and Audit Scotland guidance. Where further additional work is required, fee variations will be agreed with management and reported to the Audit Committee in our 2020/21 Annual Audit Report.

Appendix F: Additional audit information

In addition to the key areas of audit focus outlined within the plan, we have to perform other procedures as required by auditing, ethical and independence standards and other regulations. We outline the procedures below that we will undertake during the course of our audit.

Our responsibilities required by auditing standards	▸ Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. ▸ Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the College's internal control. ▸ Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management. ▸ Conclude on the appropriateness of the going concern basis of accounting. ▸ Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation. ▸ Read other information contained in the financial statements, the Audit Committee reporting appropriately addresses matters communicated by us to the Committee and reporting whether it is materially inconsistent with our understanding and the financial statements; and ▸ Maintaining auditor independence.
Purpose and evaluation of materiality	For the purposes of determining whether the accounts are free from material error, we define materiality as the magnitude of an omission or misstatement that, individually or in the aggregate, in light of the surrounding circumstances, could reasonably be expected to influence the economic decisions of the users of the financial statements. Our evaluation of it requires professional judgement and necessarily takes into account qualitative as well as quantitative considerations implicit in the definition. We would be happy to discuss with you your expectations regarding our detection of misstatements in the financial statements. Materiality determines the locations at which we conduct audit procedures and the level of work performed on individual account balances and financial statement disclosures. The amount we consider material at the end of the audit may differ from our initial determination. At this stage it is not feasible to anticipate all of the circumstances that may ultimately influence our judgement about materiality. At the end of the audit we will form our final opinion by reference to all matters that could be significant to users of the accounts, including the total effect of the audit misstatements we identify, and our evaluation of materiality at that date.
Audit Quality Framework / Annual Audit Quality Report	Audit Scotland are responsible for applying the Audit Quality Framework across all audits. This covers the quality of audit work undertaken by Audit Scotland staff and appointed firms. The team responsible are independent of audit delivery and provide assurance on audit quality to the Auditor General and the Accounts Commission. We support reporting on audit quality by proving additional information including the results of internal quality reviews undertaken on our public sector audits. The most recent audit quality report can be found at: Quality of public audit in Scotland annual report 2019/20 | Audit Scotland (audit-scotland.gov.uk). EY has policies and procedures that instil professional values as part of firm culture and ensure that the highest standards of objectivity, independence and integrity are maintained. Details of the key policies and processes in place within EY for maintaining objectivity and independence can be found in our annual Transparency Report which the firm is required to publish by law. The most recent version of this Report is for the year ended 30 June 2020: EY UK Transparency Report 2020 | EY UK

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

ey.com

Cover Paper – Internal Audit
Agenda Item A.21.3.10 (i)

University of the Highlands and Islands Moray College

Committee:	Audit Committee			
Title of Paper	Annual Fraud Update			
Brief summary of the paper:	The College/SLT can advise that it/they are unaware of any instances of fraud during AY2020/21. In addition, the College/SLT can confirm that it/they are unaware of any instances of non-compliance with regards to the relevant laws and regulations the College is required to comply with during AY20/21.			
Action requested	For noting			
Status: *(please tick ✓)*	**Reserved:**		**Non-reserved:**	X
Date paper prepared:	29 September 2021			
Date of committee meeting:	7 October 2021			
Author:	Director of Finance			
Link with strategy: Please highlight how the paper links to, or assists with: compliance partnership services risk management strategic plan/enabler other activity (e.g. new opportunity) – please provide further information.	N/A			
Equality and diversity implications:	N/A			
Resource implications: *(If yes, please provide detail)*	N/A			
Risk implications: *(If yes, please provide detail)*	Risk of fraud. Risk of non-compliance with regards to the relevant laws and regulations the College is due to comply with.			

Committee:	Audit			
Subject/Issue:	Matters arising from Cyber incident			
Brief summary of the paper:	Provides an overview of key lessons learned from the UHI Cyber Incident. Scottish Government guidance highlights the need for senior mangers to take more ownership of the cyber security risk. John Maher (UHI Director of Library and Information Systems) has attended the joint chairs committees to outline the way ahead. The key themes emerging from the incident are outlined in this paper, including local College actions.			
Action requested/decision required:	For noting.			
Status: *(please tick ✓)*	**Reserved:**	√	**Non-reserved:**	
Date paper prepared:	30th September 2021			
Date of committee meeting:	7th October 2021			
Author:	Derek Duncan			
Link with strategy: Please highlight how the paper links to, or assists with: compliance. partnership services risk management strategic plan/enabler other activity (eg new opportunity) – please provide further information.	**Risk Register ID Moray/25**: Non-compliance with relevant statutory regulations. The College must have in place effective controls to ensure personal data is kept secure and processed in line with data protection law.			
Equality and diversity implications:	Yes – the College is both a Data Controller and Data Processor of large volumes of personal data, including special category data.			
Resource implications: *(If yes, please provide detail)*	Likely impact on senior management development and cascading of practice through training to staff.			
Risk implications: *(If yes, please provide detail)*	Cyber incidents have the potential to lead to serious financial, legal and reputational damage to the College.			

Cyber Incident Response

The review of the cyber incident has identified 37 separate actions, broadly categorised across 7 key themes:

- Business continuity procedures including documenting processes and tabletop testing exercise.
- Communications both internal and external to stakeholders
- Increased resilience of systems
- Organisation wide ownership of information security (including boards and senior manager ownership)
- Reducing complexity of systems and services
- Improving staff skills, expertise, and resource
- The ICT security environment

The actions are not just for ICT leaders and technical staff, but also cover responsibilities of senior managers across the partnership with a clear need to ensure boards of management are fully briefed on developments.

The 37 actions can be briefly summarised as follows:

Theme	Summary of Action
Business continuity	Better tracking of local partner priorities.
	Continued cyber insurance and access to specialist resources.
	Document critical ICT assets and procedures.
	Ensure BCPs are better informed by incident containment and recovery processes.
	Review BCP plans and carry out tabletop exercises to test them.
Communications	Ensure use of a central web site for all users to get updates. This worked well as part of the incident response.
	Decision making on communications needs to be driven by the University (and partners), not 3rd parties with different interests.
	Ensure continued good communication between service desk staff and communication team.
	Quicker response for sign-off of emergency communications.
	Improve management of stakeholders to ensure faster and more effective communication regarding incidents.
Increase resilience	Adapt business processes for SharePoint
	Review records management considering the transfer of data to SharePoint
	SharePoint staff development
Organisation wide ownership of information security	Awareness raising for students
	Embed management of security risk at all levels of the organisation and ensure senior managers review.
	Mandatory cyber security training for staff
	Raising awareness with boards and senior managers
Reducing complexity	More resilient hosting for on-site applications
	Remove duplication of business processes and platforms
	Review business processes which use sensitive personal data

Theme	Summary of Action
Staff skills, expertise, and resource	Better joined up pooling of ICT resources to respond across the partnership
	Better understand the risks of using 3rd party service providers e.g. cloud services
	Move to cloud services has implications for skill sets as well as the legal and contractual frameworks in place. The risk needs to be understood.
	Reduce reliance on one person with specific skills used for key recovery tasks.
The ICT security environment	Document a containment plan.
	Ensure clear process for fall-back communication due to significant reliance on Microsoft Teams during incident
	Ensure the new environment covers best practice
	Implement conditional access rules for accounts e.g. restrict certain accounts to UK only.
	Implement Multi Factor Authentication for students (already in place for staff).
	Investigate managed security information event management service for early warning of threats.
	More effective arrangements to decommission old equipment and physically remove from site.
	Reduce number of physical servers to reduce energy and complexity.
	Review administration rights for staff across the partnership.
	Review backup strategies.
	Senior managers to consider options for how access to business applications can be opened up (currently restricted via the watchguard portal).
	Standardise network equipment to reduce the diversity and complexity of systems which slowed recovery.
	Improve asset management.

Actions for the College

The impact of the cyber incident on the College has been significant. The College no longer operates any corporate servers on campus and the role of local ITU staff has changed due to the way the central LIS team have recovered systems. The College no longer operates a local network operating system (Microsoft Active Directory), it is now a centralised service.

The College will support this process, with the key local actions being:

- Senior management engagement in the security risk management level at partnership and local level, this encompasses the partnership Information Security Risk Management Framework.
- Local ITU staff to become more part of the wider UHI team in terms of providing services and expertise, with appropriate training and support from senior managers.
- Keeping the board of management up to date on progress and providing assurance.
- Staff training and development (notably for SharePoint and cyber security).
- Student awareness raising.
- Business applications review, focussing on the aims of the partnership ICT strategy.
- BCP planning and testing.
- Improving the user experience of the post-cyber incident environment.

Committee:	Audit			
Subject/Issue:	Development of an Assurance Framework for the Committee			
Brief summary of the paper:	Updated briefing paper from John Maher to College boards covers the Information Security Risk Management Framework. John will join the committee and provide a verbal update.			
Action requested/decision required:	For noting.			
Status: *(please tick ✓)*	**Reserved:**	√	**Non-reserved:**	
Date paper prepared:	30th September 2021			
Date of committee meeting:	7th October 2021			
Author:	Derek Duncan			
Link with strategy: Please highlight how the paper links to, or assists with: compliance. partnership services risk management strategic plan/enabler other activity (eg new opportunity) – please provide further information.	**Risk Register ID Moray/25**: Non-compliance with relevant statutory regulations. The College must have in place effective controls to ensure personal data is kept secure and processed in line with data protection law.			
Equality and diversity implications:	Yes – the College is both a Data Controller and Data Processor of large volumes of personal data, including special category data.			
Resource implications: *(If yes, please provide detail)*	Likely impact on senior management development and cascading of practice through training to staff.			
Risk implications: *(If yes, please provide detail)*	Cyber incidents have the potential to lead to serious financial, legal and reputational damage to the College.			

University of the Highlands and Islands Information Security Risk Management Framework

Introduction

High-profile cyber-attacks are rising in prevalence, although most data breaches are the result, not of a sophisticated attack from criminals, but poor business processes or human error, for example mailing a spreadsheet of personal information to the wrong person or group. Managing information security risk to defend against cyber-attacks or avoid self-inflicted data breaches is about taking a layered approach across a range of measures from technology solutions to user education to effective policies. There is often a focus on the technical controls to manage information security risk, but it is often the people and how they work that is overlooked.

The responsibilities for information security, and therefore the management of the associated risks, are split between the university and academic partners but managed under a common information security policy framework and corresponding procedures. The majority of core IT security infrastructure sits with Learning and Information Services, but security of end user devices, local networking and local servers, local corporate information systems and data management, estates and human resources are the responsibility of the academic partner. Therefore, our information security stance is a collective effort, and our overall security position relies on consistent implementation of controls across the whole partnership.

Information security maturity model

The university is a partner in the Chief Information Security Officer (CISO) shared service, provided by HE/FE Shared Technology & Information Services (HEFESTIS), the same organisation that provides the university's data protection officer (DPO). The university has adopted HEFESTIS's information security risk management framework based on an information security maturity model of controls and a governance structure to manage those controls. This aligns with the Scottish Government's cyber resilience framework, that all public bodies in Scotland are required to comply with and report progress against.

The HEFESTIS information security maturity model has 17 control areas that cover all aspects of the information security landscape.

Table 1 Control areas

No.	Control Area	Description
1.	Organisational governance	Lack of structures, policies and processes demonstrating commitment to Information Security.
2.	Risk management	Lack of risk governance, processes and procedures, inadequate risk assessments and undefined risk treatments.
3.	Supplier management	Lack of processes and procedures for the management of partnerships with suppliers and the delivery of their products and services.
4.	Asset management	Inadequate management of hardware, software and critical infrastructure assets.
5.	Information security management	Inappropriate security measures for protecting data, services and systems.
6.	People	Lack of HR controls such as security checks and training for staff and contractors during their engagement with the University.

7.	Service resilience	The inability to maintain service delivery with current resource, the service becoming unavailable as a result leading to disruption of business operations.
8.	Access control	Inadequate account management, weak identity authentication, a lack of privilege and administrator account management.
9.	Media management	Poor management of security controls for fixed and portable storage media.
10.	Environmental security	Lack of planning for environmental threats.
11.	Physical building security	Poor physical access controls and internal security monitoring.
12.	Systems management	Lack of system management processes and procedures.
13.	Operational security	Failure to effectively monitor, manage or secure services from attack, slow/inefficient response and recovery from cyber security incidents and failing to comply with the legislative framework governing information handling leading to a critical failure of support systems.
14.	Network security	A lack of proper security configurations, updates and testing for network attached devices.
15.	Incident detection	Undetected and ignored security events leading to compromise of infrastructure. Loss, corruption or destruction of data.
16.	Incident management	Lack of incident response processes, procedures and technology.
17.	Business continuity	Lack of business continuity and disaster recovery procedures and processes.

Each of these control areas are broken down into a set of detailed controls, giving 76 in total. Table 2 shows the 5 individual controls covering Organisational Governance in relation to information security.

Table 2 Detailed Controls for Organisational Governance

1.1 Governance framework	You have effective organisational security management led at board level and articulated clearly in corresponding policies.
1.2 Leadership & responsibility	There is a board-level individual who has overall accountability for the security of networks and information systems.
1.3 Adoption of assurance standards	There is demonstrable confidence in the effectiveness of the security of the organisation's technology, people and processes.
1.4 Information Asset Register	There is a catalogue of sensitive information and data, stored with appropriate management procedures.
1.5 Audit/assurance compliance	There are in place procedures to provide assurance on the security of systems and services.

Information security risk management

There are 3 university partnership groups that meet to manage information security risk across the university:

1. Information Risk Working Group (IRWG)

The IRWG is a part of the university's formal risk management structure and provides oversight on risks and risk mitigation efforts with regards information security. The group's remit is to:

- Define the top information risks to the institution
- Maintain the Information Security Risk Register
- Maintain the Risk Control Matrix
- Devise and monitor Risk Control performance

Members include the CISO, Information Security Officer, DPOs, University Archivist and Records Manager, University Head of Internal Audit, academic partner senior managers and the Director of Learning and Information Services.

The group will direct subject specific risk management queries and actions to the relevant responsible group. If ownership is unclear the request will be directed to Partnership Council.

2. Information Security Working Group (ISWG)

The ISWG is made up of ICT professionals across the partnership with the aim of consistent implementation of technical controls to ensure best practice and retention of our current Cyber Essentials Plus accreditation in information security.

3. Risk Review Group

The role of the Risk Review Group is to support and advise Finance & General Purposes Committee, and through it the Board of Governors, on the implementation and monitoring of the risk management policy. It reviews risk management across the whole institution and will review key information security risks that threaten the achievement of the university's objectives.

Board and Senior Management ownership of cyber risk

Outcome 2 of the Scottish Government's cyber resilience framework is that businesses and organisations recognise the cyber risks and are well prepared to manage them. This can be achieved within the organisation by:

- A board-level individual who has overall accountability for the information security
- Embedding cyber resilience[1] into your governance structures, policies, and processes
- Increasing awareness and building cyber resilient behaviours of staff in all posts at all levels
- Actively managing the common information security risk embedded in your organisation's risk register

[1] Cyber resilience is the ability to deter, respond to and recover from a cyber attack in a way that minimises the impact on the business of the institution.

Information security risks

The 17 control areas translate into risks that are recorded on the information security risk register. The scoring of these risks in terms of likelihood and impact reflect the implementation of each control across the whole partnership, recognising the interconnectedness of the partnership, meaning we are only as strong as the weakest link.

The information security risk register is maintained by the Information Risk Working Group and the risks are included in the university's risk register, which is monitored by the Risk Review Group.

Academic Partner and University Common Risk

In addition to the 17 risks each academic partner and the university have a common information security global risk in their organisation's risk register which is about culture, people and processes, something senior managers and boards leading the organisation can influence and manage directly.

Relevant and necessary information security accreditation

Cyber Essentials Plus

Currently the Scottish Government requires all public bodies, including universities and colleges to hold Cyber Essentials Plus accreditation. The university obtained this, with a whole of institution scope, in 2019. It is subject to an annual external verification audit.

ISO27001

The university does not hold ISO27001 and there are no plans currently to obtain it. There have been examples where grant funding has required assurance that elements of the ISO27001 framework, or equivalent controls are in place, and this has been provided where necessary.

Appendix 1 Common information security global risk

The impact of an information security incident can be considerable. Dundee and Angus College had to close for 7 days at the beginning of February 2020, following a phishing instigated attack that saw all their data and backups encrypted by ransomware, some of which, including student assessments, were never recovered. Both Newcastle and Northumbria Universities suffered a similar attack at the start of September 2020.

There are several risks on the university partnership's information security risk register that look at the technical implementation of controls that mitigate the impact of a cyber security event. However, it is often the people and how they work that is overlooked. Each academic partner and the university has a common information security risk in their organisation's risk register which is about people and processes, and it is something you in your role of leading the organisation can influence and manage.

Common risk description

"Institutional, personal, and sensitive data and/or services are disrupted, corrupted, lost, stolen, or misused through serious inappropriate usage of IT systems or data, by internal users of the university partnership or external actors."

Developing a positive cyber security culture

Mitigating this risk is not about technical controls but more about the attitude to information security risks within working practices, staff training and the culture that you can influence within your organisation. The risk of a member of staff losing a list of student contact details or sharing data by accident to the wrong people through an incorrectly addressed email is mitigated with better information security awareness training and a review of common work practices. Is there a better way of accessing student details or sharing data without using email?

Establishing and maintaining a healthy culture, in any part of your organisation, is about putting people at the heart of structures and policies. However, when it comes to cyber security, there is sometimes a tendency to focus almost exclusively on technical issues and to overlook the needs of people and how they really work.

This rarely results in success. We know, for example, that when official policy makes it hard for someone to do their job, or when a policy is no longer practical, that people find workarounds and 'unofficial' ways of carrying out tasks. Or that there are long held practices regarding the sharing and use of personal data that expose us to greater risks now we have moved online, using new tools to share data, and this is heightened now we're working at home.

Without a healthy security culture, staff will not engage with cyber security, so you will not know about these workarounds or unofficial approaches. Not only will you have an inaccurate picture of your organisation's cyber security, but you will also miss the opportunity for valuable staff input into how policies or processes could be improved.

Causes

The causes of this risk include:

- Lack of controls around information security and data protection.
- Poor staff awareness of existing policies and procedures and best practice with regards information security.
- Inappropriate business processes or practices that expose sensitive data to loss or misuse.

- Malicious, illegal, or unintentional data leakage through phishing, insecure data transfer methods or sharing with unauthorised users.
- Lack of appropriate background security checks during recruitment.
- Poor information classification and information asset management.
- Weak estates access control, especially to areas where personal and sensitive data is managed.
- Loss of an insecure corporate or personal device or removable media with corporate data on it while on or off campus.
- Running out of date software and devices due to budget constraints or personal choice.
- Larger than normal numbers of system users with widely distributed access rights and permissions given the size and structure of the university partnership.
- Badly configured technical controls e.g. poor patching regime, anti-virus out of date, corporate mobile devices not encrypted.
- In appropriate disposal of IT equipment.

Impacts/Evidence

The impacts of this risk can be:

- Disruption of access to important information for short or sustained period.
- Permanent loss of unbacked up data through data corruption or malicious ransomware encryption.
- Prohibitive fines imposed by ICO.
- Adverse press coverage.
- Impact of disrupted, lost or stolen important information and services:
    - loss of reputation, confidence, and trust
    - financial penalties
    - official sanction
    - loss of business
    - poor performance in student KPIs e.g. NSS score
    - costs, resources, and time taken to manage and rectify the incident

What should the Board and Senior Management do?

Lead by example

You set the tone when it comes to cyber security. Make information security a regular agenda item and engage with your experts, both within your organisation and the university. Lead by example and champion cyber security within your organisation. There are often stories of senior leaders ignoring security policies and processes, or of asking for 'special treatment' in some way (such as requesting a different device to those issued as standard). This tells everyone else in the organisation that perhaps you do not consider the rules fit for purpose, and/or that it is acceptable to try to bypass them. If policies don't work for you as a Board member or Senior Manager (that is, if you find yourself doing something different to get your job done more easily), then there is a good chance they aren't working for others either. If it seems that the policy is having a detrimental effect on the organisation, work with policy makers to adapt it. Culture takes time and concerted effort to evolve. Do not assume that because the Board has endorsed a security posture that it will automatically cascade down throughout the organisation.

Develop a 'just culture'

Developing a 'just culture' will enable the organisation to have the best interaction with staff about cyber security. Staff are encouraged to speak up and report concerns, appropriate action is taken,

and nobody seeks to assign blame. This allows staff to focus on bringing the most benefit to the organisation rather than focusing on protecting themselves.

Mitigations to implement and monitor

Specific risk mitigations your organisation should implement include:

- Ownership and proactive monitoring of cybersecurity risks by university and academic partner senior management level on a regular basis, including ongoing monitoring of the effectiveness of the controls implemented to provide risk mitigation.
- Implement the university partnership's common information security policy framework by:
    - Contextualising them for your organisation's structure and operation.
    - Assigning ownership of key responsibilities to named staff.
    - Regularly reviewing progress and performance against the policies aims.
- Have a complete and up to date information asset register.
- Question and validate business processes and practice where personal data is handled to ensure sensitive personal data is secured appropriately, handled correctly, and accessed carefully by approved users.
- Implement a tidy desk policy and enforce it.
- Mandated information security training for all staff and increased staff awareness of information security issues.
- Information security embedded as a core aspect of all staff job roles and candidates are screened appropriately during recruitment.
- Estates security is reviewed with information security in mind and appropriate access controls implemented.
- Business continuity plans in place for cyber-attack and information breach response procedures are rehearsed.
- Coordinated data governance practitioners and implementation of output from GDPR preparations.
- Open culture promoting the reporting of potential data security issues for investigation.

Additional Help

The university employs experts to help us manage information security. These include a Chief Information Security Officer (CISO), provided as part of a sector wide shared service like DPO Share, and an Information Security Officer, looking after operational aspects of information security. As part of the CISO Share approach we now have 2 groups that are looking at information security across the university partnership:

- Information Security Working Group: Made up of ICT professionals across the partnership with the aim of consistent implementation of technical controls to ensure best practice and retention of our current Cyber Essentials Plus accreditation in information security.
- Information Risk Working Group: Oversight of information risk across the partnership looking at all aspects of operation. Members include CISO, Information Security Officer, DPOs, University Archivist and Records Manager, University Head of Internal Audit, academic partner senior managers and the Director of Learning and Information Services.

Along with the Director of Learning and Information Services, the CISO and Information Security Officer are happy to assist you and your team in all aspects of information security from awareness raising to review and suggested mitigation and controls.

Appendix 2 Resources

Introduction to cyber security for Board members - NCSC.GOV.UK

Scottish Government's Cyber Resilience Strategy (www.gov.scot)

About Cyber Essentials - NCSC.GOV.UK

HEFESTIS CISO Shared Service (hefestis.ac.uk)

University Information Security Policies (sharepoint.com)

LIS IT security web pages (uhi.ac.uk)

LIS services overview

University of the Highlands and Islands
Moray College

Committee:	Audit			
Subject/Issue:	GDPR Update – full year statistics			
Brief summary of the paper:	Provides a summary of annual GDPR statistics, including breaches reported to the Information Commissioner's Office (ICO). No statutory data breaches were recorded.			
Action requested/decision required:	For noting.			
Status: *(please tick ✓)*	**Reserved:**	√	**Non-reserved:**	
Date paper prepared:	30th September 2021			
Date of committee meeting:	7th October 2021			
Author:	Derek Duncan			
Link with strategy: Please highlight how the paper links to, or assists with: compliance partnership services risk management strategic plan/enabler other activity (eg new opportunity) – please provide further information.	**Risk Register ID Moray/25**: Non-compliance with relevant statutory regulations. The College must have in place effective controls to ensure personal data is kept secure and processed in line with data protection law.			
Equality and diversity implications:	Yes – the College is both a Data Controller and Data Processor of large volumes of personal data, including special category data.			
Resource implications: *(If yes, please provide detail)*	All required resources are in place.			
Risk implications: *(If yes, please provide detail)*	Data protection breaches can lead to serious financial and reputational damage to the College.			

1. GDPR Annual Update

The Audit committee will now only be updated with any significant data protection events and the annual update on overall incidents included in this paper.

This update covers the College financial year ending 31st July 2021, with the previous 2 years data provided for comparison.

Overall, there has been a reduction in reported incidents, with a slight reduction in actual data breaches confirmed:

Year	#Incidents	#Breaches Confirmed	#Reported to ICO
18/19	19	11	1
19/20	20	12	2
20/21	11	9	1
Grand Total	**50**	**32**	**4**

20/21 Overview

It is unclear if the reduction in incidents was due to the global pandemic and staff working from home. The UHI cyber incident may have contributed due to:

- Unavailability of Internal systems which were shutdown from 5th March, significantly impacting data processing activities.
- Almost all file systems not being accessible during the incident response which were eventually transferred to SharePoint services.
- Change in staff practice, with emails used to share links to secure data instead of the raw data being shared directly via file attachments. Email has consistently been the weakest link in terms of data security overall.

2. UHI Cyber Incident

The UHI Cyber Incident is not recorded in these statistics. The University partnership DPO reported an availability breach to the ICO on the 5th of March 2021 and to date, there is no evidence of any data breach involving College data.

3. ICO Reporting

None of the incidents reported to the ICO resulted in any enforcement action. Decisions on referring incidents to the ICO are based on incident reviews with the College's independent Data Protection Officer.

4. Subject Access Requests (SAR)

The College received one SAR request in session 2018/19.

5. Right to Erasure

The College has not received any right to erasure requests.

Committee:	Audit			
Subject/Issue:	Status of all College Policies, Plan for Review and Updating			
Brief summary of the paper:	This paper provides a plan for policy updates in session 20/21. The College continues to recover from two business continuity events which has meant that review policy reviews have had lower priority. Clearing the full backlog throughout session21/22 is not achievable at present, but the plan does target those policies most in need of attention. For many policies, the review process will be straightforward since some are regional and only require local endorsement, others need different levels of change.			
Action requested/decision required:	For noting.			
Status: *(please tick ✓)*	**Reserved:**		**Non-reserved:**	√
Date paper prepared:	30th September 2021			
Date of committee meeting:	7th October 2021			
Author:	Derek Duncan			
Link with strategy: Please highlight how the paper links to, or assists with: compliance. partnership services risk management strategic plan/enabler other activity (eg new opportunity) – please provide further information.	**Risk Register ID Moray/18**: Non-compliance with relevant statutory regulations.			
Equality and diversity implications:	Yes – a key statutory requirement which underpins all operational areas of the College.			
Resource implications: *(If yes, please provide detail)*	Significant – impact of losing 2 Directors and likely extended period of time to recruit new post will have an impact.			
Risk implications: *(If yes, please provide detail)*	Non-compliance due to deficient polices, training or leadership carries a risk to staff, learners and 3rd parties, as well as possible legal and reputational damage to the College.			

Policy Update

The response to the pandemic and cyber incident significantly impacted the policy review process, with senior managers focussing on business continuity tasks to close out the last session and prepare the College for the new academic year. There are also temporary staffing challenges within the Strategic Leadership Team which has been considered in terms of the plan for 21/22.

A realistic plan has been developed which prioritises policies most in need of update whilst delaying lower-risk policies.

Risks

The failure to keep policies up to date creates risk and has been managed throughout the pandemic.

The College website guidance for complaints was updated to reflect statutory changes which came into effect from 1st April. This is a regional procedure which purely requires internal approval and therefore is not considered high-risk at this time.

There are further risks due to the global pandemic which may create additional pressures on staff depending on the type of response required.

Policy Overview

The College register contains 82 policies, procedures and strategy documents and of these, 54 are currently not due for review or are new or on hold (also covered later in this paper).

This leaves 27 policies now overdue for review.

In practical terms, the plan outlines a total of 17 which can be reviewed this session covering those more than 9 months overdue or where they are considered a priority for review.

There are no HR policies outstanding since these are reviewed by a separate group, including trade union representatives which is reported to the Staff Governance Committee.

The responsibility for the 17 policies to be reviewed rests with the Director of Finance (DoF) and Director of Information, Planning and Student Support (DIPSS). 4 of the policies are regional and only require approval rather than any development work.

The 17 policies planned for review, the approving committee and meeting date are provided in the table below:

Policy/Procedure to be reviewed	College or Regional?	Approving Committee	Resp. Director	Committee Date
Fraud Policy and Response Plan	College	Audit	DoF	07/10/2021
Gift, Hospitality, Entertainment Policy	College	Audit	DoF	17/02/2022
Risk Management Policy and Procedures	College	Audit	DoF	17/02/2022
Financial Procedures	College	F & GP	DoF	10/03/2022
Financial Regulations	College	F & GP	DoF	10/03/2022
Procurement Strategy	College	F & GP	DoF	10/03/2022
Smoke-free Policy	College	F & GP	DIPSS	10/03/2022
University Partnership Records Management Policy and Procedures	Regional	F & GP	DIPSS	09/06/2022
Work Placement Policy	Regional	F & GP	DIPSS	09/06/2022
Estates Strategy	College	F & GP	DIPSS	09/06/2022
Complaints Procedures	Regional	Full Board	DIPSS	24/03/2022

Policy/Procedure to be reviewed	College or Regional?	Approving Committee	Resp. Director	Committee Date
Corporate Parenting Plan	College	Full Board	DIPSS	24/03/2022
Student Attendance Policy and Procedures	College	LTQ	DIPSS	11/11/2021
Student Confidentiality Policy	College	LTQ	DIPSS	11/11/2021
Student Disclosure Policy	College	LTQ	DIPSS	17/03/2022
Student Induction Policy	College	LTQ	DIPSS	17/03/2022
Tertiary Equality and Diversity Policy	Regional	LTQ	DIPSS	17/03/2022

Policies Updates on Hold

The following policies are on hold and the reasons are outlined in the table below:

Policy	Reason for Hold
Commercialisation Strategy	This has been outstanding for some time and requires further discussion.
Estates Asset Procedures	New Facilities Manager to investigate preferred approach.
Support for Consultation Procedure	Awaiting update on national bargaining and UHI policy.
Job Evaluation & Regrading Procedure	Awaiting update on national bargaining and UHI policy.
Staff Review Procedure	Awaiting update on national bargaining and UHI policy.
Student Advice, Personal Development Planning and Guidance Policy	To be replaced with new regional policy
Student Attendance Policy and Procedures	Regional approach to be adopted.

MORAY COLLEGE UHI

Fraud Policy and Response Plan Policy

Status	Updated for Approval
Version Date and Number	V1.2 21/009/21
Approved by	Audit Committee (Due date: October 2021)
Responsibility for Policy	Director of Finance
Responsibility for Implementation	Director of Finance
Responsibility for Review	Director of Finance
Date for Review	October 2021

Please ask if you, or someone you know, would like this document in a different format or language.

Revision Date & Change Log

Date of Revision	Brief Description of Change	Date Approved
22 Nov 18	V1.0 Initial draft for review (and approval)	
Feb 2021	V 1.1 Updated to include NFI information.	
Sep 2021	V 1.2 Updates made to legislation	

Table of Contents

1. Introduction

The College is committed to providing a high standard of service, accountability, probity and openness. An important aspect of this is having an anti-fraud and related criminal offences policy which commits the College to ensuring that the risk of fraud is reduced and that fraud is deterred, detected and investigated.

This policy outlines the College's underlying objectives and approach to fraud prevention. It explains how suspicions should be reported and acted upon, documents the roles and responsibilities of the key parties and details the College's Fraud Response Plan.

In line with the Public Interest Disclosure Act, the Board of Management wishes to encourage staff or the public, having reasonable suspicion of fraud to report the incident. It is the policy of the Board of Management that no staff member should suffer in any way by reporting in good faith any reasonably held suspicions.

The college recognises that it is already subject to a high degree of external scrutiny of its affairs by a variety of parties. These include the Board of Management, Internal and External Auditors, Audit Scotland, the Scottish Funding Council ("SFC"), the Regional Strategic Body ("RSB"), HM Revenue and Customs, staff, students and the general public.

2. Definition of Fraud

The term "fraud" will cover fraud, theft and other illegal acts involving corruption, bribery, dishonesty or damage to property, except where the context indicates otherwise. It is where one or more individuals or entities obtain an unjust or illegal advantage/cash/benefit through an intentional act which usually includes deception, e.g.;

- Misappropriation of cash;
- Inappropriate expense claims;
- Manipulation of student data to generate additional income;
- Access to confidential data by breach of computer systems (e.g. bank account details);
- Awarding contracts where there is personal advantage.

The College recognises that some HR and academic issues could also be classified as fraud and where these are so classified by the Principal these will also be dealt with under this policy and subsequent Response Plan.

3. Responsibilities

All Staff Members

This policy applies to all College staff and members of the Board of Management.

It is a fundamental principle that all College staff and board members should act honestly and with integrity to safeguard the public resources for which they are responsible.

It is the responsibility of each individual to familiarise themselves with the rules detailed in this policy and to comply with them.

It is the responsibility of all staff to safeguard the assets of the Board of Management. Assets include information and goodwill, as well as property.

Director of Finance

It is the responsibility of the Director of Finance to maintain adequate and effective internal controls to facilitate detection of fraud, and to review this policy either every three years or immediately if impacted by any changes to the law.

Responsibility for investigating fraud/theft has been delegated to the Director of Finance.

The Director of Finance will also be responsible for informing third parties such as the Scottish Funding Council, internal and external auditors or the police, where appropriate.

The Director of Finance shall use his/her judgement in determining if the Principal and other Directors/the Strategic Leadership Team of the College should be informed.

The Director of Finance shall normally inform the Convener of Audit at the first opportunity and delegate to the Internal Auditors, responsibility for leading any investigation whilst retaining overall responsibility.

Where a member of staff is to be interviewed or disciplined, the Director of Finance and/or the Internal Auditors shall consult and take advice from the Director of Human Resources and Organisational Development.

Where the incident is considered to be subject to either local or national controversy and publicity, then the Board of Management, RSB and the SFC should be notified (in addition to the External Auditors) before the information is made public.

It shall be necessary to categorise the irregularity prior to determining the appropriate course of action. Two main categories exist:

- Theft, burglary and isolated opportunist offences; and,
- Fraud, corruption and other financial irregularities.

The former will be dealt with directly by the police whilst the latter may require disclosure under the Further and Higher Education (Scotland) Act 2005.

Director of Human Resources and Organisational Development

The Director of Human Resources and Organisational Development shall advise those involved in the investigation in matters of employment law and in other procedural matters, such as disciplinary and complaints procedures.

Board of Management

It is the responsibility of the Board of Management, through College management, to ensure that a risk awareness culture exists, that staff are aware of the above requirements and that appropriate reporting arrangements are in place.

4. National Fraud Initiative

The College participates in the National Fraud Initiative (NFI) to assist in the prevention and detection of fraud.

The NFI in Scotland is a counter-fraud exercise led by Audit Scotland, and overseen by the Cabinet Office for the UK as a whole. It uses computerised techniques to compare information about individuals held by different public bodies, and on different financial systems that might suggest the existence of fraud or error.

Further information about the NFI can be found at www.audit-scotland.gov.uk/our-work/counter-fraud

5. Response Plan

5.1 Introduction

The fraud response plan sets out the College's procedures for ensuring that allegations and reports of fraud are properly investigated, are considered in a consistent and fair manner and that prompt and effective action is taken to minimise the risk of any losses and reduce any adverse effects. It also makes a clear statement that fraud will be treated very seriously.

The following sections describe the Board of Management's intended response to a reported suspicion of fraud/theft. These procedures are designed to allow for evidence gathering and collation in a manner that will facilitate informed initial decisions, while ensuring that any evidence gathered will be admissible in any criminal or civil action. Each situation is different, therefore, the guidance must be considered carefully in relation to the specific circumstances of each case before action is taken.

Under no circumstances should a member of staff speak or write to representatives of the press, TV, radio or to another third party to whom the disclosure of information would not be a "protected disclosure" within the terms of the Public Interest Disclosure Act, about a suspected fraud/theft without the express authority of the Principal.

Care needs to be taken that nothing is done that could give rise to an action for defamation of character.

5.2 Reporting Fraud

The Director of Finance is the "Nominated Officer" to whom reports of any suspicion of fraud, theft or corruption should be made.

For incidents involving the Director of Finance, the Chair of the Board of Management will be informed and will either adopt the role or nominate a "Nominated Officer".

The Nominated Officer shall be trained in the handling of concerns raised by staff. The Nominated Officer shall, wherever possible, respect any request for anonymity or confidentiality providing that in doing so, that it is consistent with the overall aims and objectives of this policy and the principles of natural justice.

All reported suspicions must be investigated as a matter of priority to prevent any further potential loss to the Board of Management.

The Nominated Officer shall maintain a log of any reported suspicions. The log will document with reasons the decision to take further action or to take no further action.
To justify such decisions the nominated officer shall retain as necessary, "confidential" files of evidence gathered to arrive at a decision. These files will be securely held with limited access.

The log will detail any actions taken and conclusions reached with appropriate cross-referencing to any file held. The log should be reviewed annually by the Internal Audit function, who will report to the Audit Committee on any significant matters.

The Nominated Officer should consider the need to inform the Board of Management, RSB, Internal Auditor, External Auditor and police of the reported incident.

In doing so, the Nominated Officer should take cognisance of the following guidance:

- Inform and consult the Principal at the first opportunity in all cases where the loss may exceed the delegated limit (or such lower limit as the Board of Management may determine) or where the incident may lead to adverse publicity.

- It is the duty of the Nominated Officer to notify the Board of Management immediately of all losses where fraud/theft is suspected.

- The Internal Auditors should normally be informed immediately in all but the most trivial of cases.

- If a criminal act is suspected, particularly fraud or corruption, it is essential that there is the earliest possible consultation with the police. In any event, the police should be contacted before any overt action is taken which may alert suspects and precipitate the destruction or removal of evidence. This includes taking action to stop a loss or tighten controls.

- At the stage of contacting the police the Nominated Officer should contact the Director of Human Resources and Organisational Development to initiate the suspension of the employee pending an enquiry.

All such contacts should be formally recorded in the log.

5.3 Managing the Investigation

The Nominated Officer will appoint a manager to oversee the investigation. Normally the manager will be the Chief Internal Auditor. The circumstances of each case will dictate who will be involved and when.

The manager overseeing the investigation (referred to hereafter as the "Investigating Manager") should initially:

- Initiate a Diary of Events to record the progress of the investigation.

- If possible, determine if it is a fraud investigation or another criminal investigation. In practice, it may not be obvious if a

criminal act has taken place. If a criminal event is believed to have occurred, the police, external auditor and the Board of Management should be informed if this has not already been done.

If a criminal offence is believed to have occurred, the Investigating Manager should consider whether it would be more appropriate for the police to handle the investigation. Under these circumstances, internal enquiries and disciplinary proceedings would not be initiated until the conclusion of criminal proceedings.

A formal internal investigation to determine and report upon the facts should be carried out. This should establish:

- The extent and scope of any potential loss.
- Any disciplinary action needed.
- The criminal or non-criminal nature of the offence, if not yet established.
- What can be done to recover losses.
- What may need to be done to improve internal controls to prevent reoccurrence.

This report will normally take the form of an Internal Audit Report to the Board of Management's Audit Committee.

Where the report confirms a criminal act and notification to the police has not yet been made, it should now be made.

Where recovery of a loss to the Board of Management, arising from any act (criminal or non-criminal), is likely to require civil action, the College should seek legal advice from its legal representatives.

The report of the investigation should form the basis of any internal disciplinary action against a staff member. The conduct of internal disciplinary action will be assigned to the Director of Human Resources and Organisational Development who shall gather such evidence as necessary.

5.4 Disciplinary/Dismissal Procedures

The employee(s), who is the subject of any investigation, should be suspended pending the results of any internal investigation or criminal proceedings. This should be carried out in line with the College's conduct procedures.

The conduct procedures must be followed in any disciplinary action taken by the Board of Management against an employee (including dismissal).

This may involve the Investigating Manager recommending a disciplinary hearing to consider the facts, the results of the investigation and take appropriate action against the employee.

5.5 Gathering Evidence

It is not possible for this policy to cover all the complexities of gathering evidence. Each case must be treated according to the circumstances of the case taking professional advice as necessary.

As general guidance, the "International standard on auditing (UK) 500" (Jan 2020) should be referred to. In line with the Standard the Investigating Manager should at all times seek to maximise the reliability of audit evidence.

If a witness to the event is prepared to give a written statement, it is best practice for an experienced member of staff, preferably from Human Resources, to take a chronological record using the witness's own words. The witness should sign the statement only if satisfied that it is a true record of his or her own words.

At all stages of the investigation any discussions or interviews should be documented and where possible agreed with the interviewee.

Physical evidence should be identified and gathered together (impounded) in a secure place at the earliest opportunity. An inventory should be drawn up by the investigating Manager and held with the evidence. Wherever possible replacement or new documents, etc. should be introduced to prevent access to the evidence.

If evidence consists of several items, for example a number of documents, each one should be tagged with a reference number corresponding to the written records.

5.6 Interview Procedures

Interviews with suspects should be avoided until the formal conduct hearing. The Investigating Manager should wherever possible attempt to gather documentary and third party evidence for the purposes of the report. If an employee insists on making a statement, it should be signed and dated and include the following:

"I make this statement of my own free will, I understand that I need not say anything unless I wish to do so and what I say may be given in evidence."

Informal contact with the police should be made at an early stage in any investigation to ensure that no actions are taken that could prejudice any future criminal case through the admissibility of evidence, etc.

5.7 Disclosure of Loss from Fraud

A copy of the Fraud report in appropriate format must be submitted via the RSB to the SFC. External Audit should also be notified of any loss. The Fraud report submitted annually to the Audit Committee should include any loss with appropriate description.

Management must take account of the permitted limits on writing off losses including losses that require formal approval.

5.8 Police Involvement

It shall be the policy of the Board of Management that wherever a criminal act is suspected the matter will be immediately notified to the police.

The Nominated Officer will decide at what stage the police are contacted.

The Nominated Officer and Investigating Manager should informally notify police of potential criminal acts to seek advice on the handling of each investigation at an early stage in the investigation.

5.9 Press Release

To avoid potentially damaging publicity to the College and/or to the suspect, the Principal, on behalf of the Board of Management should prepare at an early stage a Press Release giving the facts of any suspected occurrence and any actions taken to date e.g. suspension, although the name of any staff member suspended pending investigation should not be released to the press.

6. Resourcing the Investigation

The Nominated Officer will determine the type and level of resource to be used in investigating suspected fraud. The choices available will include:

- Internal staff from within the College
- Internal Auditor
- External Auditor
- Specialist Consultant
- Police

In making a decision the Nominated Officer should consider independence, knowledge of organisation, cost, availability and the need for a speedy investigation.

Any decision must be shown in the log held by the Nominated Officer. A decision to take "No Action" will not normally be an acceptable option except in exceptional circumstances.

In any case involving a suspected criminal act it is anticipated that police involvement will be in addition to an alternative resource.

7. The Law and its Remedies

7.1 Criminal Law

The Board of Management shall refer all incidences of suspected fraudulent or criminal acts to the police for decision by the Procurator Fiscal as to any prosecution.

7.2 Civil Law

The Board of Management shall refer all incidences of loss through proven fraudulent or criminal act to their legal representatives to determine whether the loss can be recovered by civil action.

8. Review

The College will utilise the investigative report to review and improve its internal control systems.

9. References

Both internal and external references are listed in Appendix A.

Appendix A

Internal References

- Board of Management Code of Conduct
- Code of Conduct for College Employees
- Capability and Conduct Procedure for College Employees
- Financial Regulations
- Financial Procedures
- Capability and Conduct Procedure for College Employees
- Whistleblowing Procedures
- Gift, Hospitality and Entertainment Policy
- Board of Management Declaration of Interest
- Board of Management Code of Conduct

External References

- Public Interest Disclosure Act (As amended)
- Fraud Act 2006
- Bribery Act 2010
- National Fraud Initiative (NFI) – Audit Scotland