

# BOARD OF MANAGEMENT

## Audit & Risk Committee

Tuesday 9 March 2021 at 5.00pm  
In Microsoft Teams

---

### AGENDA

1. **WELCOME**
2. **APOLOGIES**
3. **DECLARATIONS OF INTEREST**
4. **MINUTE OF THE PREVIOUS MEETING –**  
8 December 2020 Paper A for approval
5. **MATTERS ARISING** Paper B for noting
6. **COVID 19 UPDATE** Verbal update    JC/ST
7. **INTERNAL AUDIT**
  - 7.1 National Fraud Initiative Paper C for approval    HL
  - 7.2 Systems Development / Implementation Paper D for approval    HL
  - 7.3 20/21 Progress Report Paper E for noting    HL
  - 7.4 Follow Up Summary Paper F for information    JC
8. **EXTERNAL AUDIT** Verbal Update    AS
9. **STRATEGIC RISK & COVID REGISTER** ST
  - 9.1. Strategic Risk Register Paper G for approval
  - 9.2. COVID Risk Register Paper H for approval
10. **INFORMATION AND CYBER SECURITY RISK** Paper I for information    DR  
(David Robertson, our HEFESTIS shared Chief Information Security Officer will attend)
11. **DATE OF NEXT MEETING – Tuesday 18 May 2021.**

**BOARD OF MANAGEMENT**

**Audit & Risk Committee**

**Tuesday 9 March 2020**

---



**Minute of Previous Meeting – 8 December 2020**

**PAPER A**

# **BOARD OF MANAGEMENT**

## **Audit and Risk Committee Meeting**

### **Tuesday 8 December 2020**



*Draft confirmed by Chair*

---

Minute of the Audit & Risk Committee meeting held on Tuesday 8 December at 4.30pm via MS Teams

**PRESENT:** G Robertson (Chair Audit) M Williamson  
H Honeyman K Keay  
M Thomson P Milne

**IN ATTENDANCE:** J Carnegie (Vice Principal) T D'All (Principal's/Board Chair PA)  
S Taylor (Vice Principal) D Archibald (Henderson Loggie)  
A Kerr (Audit Scotland) S Inglis (Henderson Loggie)  
R Smith (Audit Scotland)

#### **1. WELCOME**

G Robertson welcomed members of the Audit Committee.

It was confirmed that an independent meeting with audit representatives had been held directly prior to the meeting.

#### **2. APOLOGIES**

Apologies were received from T Pirie

#### **3. DECLARATIONS OF INTEREST**

G Robertson noted his role as Chair of the Board for Gardyne Theatre Limited. There were no other declarations of interest.

#### **4. MINUTE OF AUDIT & RISK COMMITTEES – 22 SEPTEMBER 2020**

The minutes of the Audit Committees meeting held on 22 September 2020 was approved as a correct record.

#### **5. MATTERS ARISING**

Matters arising from previous meeting were closed.

## 6. STRATEGIC RISK REGISTER

S Taylor summarised the proposed changes to the Strategic Risk Register and deletion of the risk around structure changes. Work on monitoring the risks associated with Brexit were noted.

In response to a query S Taylor noted that the high-risk likelihood noted in respect of 3.3 “Legal actions; serious accident; incident or civil/criminal breach” related to the risk without the mitigations in place.

The COVID 19 Risk Register was noted and S Taylor summarised reduced scoring due to experience in respect of the risks around the negative publicity of any COVID outbreak and the potential impact of changes to awarding body quality arrangements.

G Robertson enquired about staff absence and it was confirmed by S Taylor that this was lower than usual at that time of year. This was likely due to offsite working, social distancing and improved hand and respiratory hygiene.

G Robertson asked about the number of staff on site and J Carnegie confirmed that a recent request for this information from the Scottish Government returned the number as approx. 300 people.

H Honeyman noted an announcement today from the Scottish Government around the cancelling of Highers and Advanced Higher for AY 2020/21 and asked how this would impact on the work of the College. S Taylor confirmed in terms of Higher this was a small number of students (approx. 400) with no Advanced Higher programmes currently being offered. S Taylor noted that as this was a recent announcement the College is awaiting further guidance but would expect the situation to be similar to that of National 5 provision.

The Strategic and COVID Risk Registers were approved.

## 7. DRAFT AUDIT COMMITTEE REPORT TO BOARD

G Robertson summarised the work undertaken by the Audit & Risk Committee over the preceding year and as included in the Draft Report to the Board.

The Committee noted that they were satisfied with the content of the report and approved this for submission to the December Board. **T D’All to progress.**

## 8. INTERNAL AUDIT REPORTS

### 8.1 Student Activity

S Inglis summarised the report on student activity (credits) highlighting that this was a prescribed audit to fulfil SFC requirements. S Inglis confirmed the “clean opinion” to SFC.

S Inglis highlighted the increase in Distance Learning due to COVID-19, an increase of 1100 credits, due to the upsurge in digital technology training due to the increased use of ICT systems including MS Teams, Webinars etc for students working remotely. Guidance was sought from SFC who were happy to accept these courses for AY 2019/20.

The Committee welcomed the report and the positive comment on the work undertaken to achieve the ‘clean’ outcome. The report was approved.



## 8.2 Student Funding

S Inglis summarised the audit report on student support funds (Bursary, EMA and Hardship), confirming that this conformed to SFC requirements in relation to the range of funds identified with a “clean certificate”.

The only observation that S Inglis noted was SFCs requirement for spot check of the EMA (100% attendance required) and that due to the cyber-attack at the start of the year some of the data was missing. It was confirmed that checking of data after the cyber-attack confirmed that appropriate arrangements were in place.

The report was approved.

## 9. Audit & Risk Follow-Up Summary

J Carnegie summarised the Follow-Up Summary document highlighting a date change for the Learner Engagement Strategy to August 2021. J Carnegie stated that it was not felt to be appropriate to finalise this until ‘post COVID’ learning and study arrangements were clearer.

J Carnegie noted that the questions with the Digital Skills Capability Assessment were no longer relevant as Digital Capability has developed and evolved significantly due to COVID.

J Carnegie sought approval to marked this “action” as complete. The Committee agreed this.

Actions in respect of the Cyber-attack report were noted and it was confirmed that good progress had been made.

G Robertson asked about the reference to the ‘Red Forest’ technique asked if there was any risk associated with the alternative being progressed. J Carnegie noted that as the Head of ICT was not at the meeting, she would request information on this be provided for the next Audit & Risk Meeting in the New Year **J Carnegie to progress.**

## 10. DATA BREACH REPORTING

J Carnegie confirm there were no reportable Data Breaches.

## 11. DATE OF NEXT MEETING

The next Audit & Risk Committee meeting was confirmed as: **Tuesday 9 March 2021 at 5.00pm via MS Teams**

### Action Point Summary

Action	Responsibility	Date
Update on any additional risk associated with decision not to progress with ‘Red Forest’ technique.	J Carnegie	9 March 2021

# BOARD OF MANAGEMENT

## Joint Audit and Risk/Finance and Property Committee Meeting

Tuesday 8 December 2020



*Draft confirmed by Chair*

---

Minute of the Joint Audit and Finance & Property Committee meeting held on Tuesday 8 December 2020 at 5.15m via MS Teams

**PRESENT:**

G Robertson (Chair Audit)	Steven Mill (Chair Finance & Property)
A McCusker	M Williamson
H Honeyman	K Keay
M Thomson	S Hewitt
D Fordyce	B Carmichael
D Mackenzie	S Stirling
P Milne	N Lowden

**IN ATTENDANCE:**

J Carnegie (Vice Principal)	Julie Grace
S Taylor (Vice Principal)	T D'All (Principal's/Board Chair PA)
A Kerr (Audit Scotland)	R Smith (Audit Scotland)
D Archibald (Henderson Loggie)	S Inglis (Henderson Loggie)
Billy Grace (Head of Estates)	B Ferguson (Head of Finance)

### 1. WELCOME

G Robertson welcomed members of the Finance and Property Committee to the joint meeting.

### 2. APOLOGIES

Apologies were received from, T Pirie & G Bisset

### 3. DECLARATIONS OF INTEREST

G Robertson noted his role as Chair of the Board for Gardyne Theatre Limited. here were no other declarations of interest.

### 4. ANNUAL REPORT ON INTERNAL AUDIT

D Archibald delivered a summary of the year's work including a summary of the individual reports noting that the annual operating plan for 2019/20 showed several changes agreed by the Audit & Risk Committee to the allocation set out in the original Strategic Plan.

D Archibald confirmed that the Audit Plan had been delivered intact and that there were no issues identifying major internal control weaknesses noted from the internal audit work carried out during the year. Although the January 2020 cyber-attack on the College resulted in some limitations on scope, within the testing of Procurement and Creditors / Purchasing, D Archibald confirmed that they were comfortable that, overall, sufficient evidence was available to provide robust findings on the agreed audit scope.

S Mill noted that the positive review but queried the “satisfactory” grading for the great work undertaken by the ICT Team and asked if this was too harsh. D Archibald noted that while there were no significant control weaknesses, the cyber-attack and the loss of data had contributed to this audit outcome.

S Mill enquired about the scope for the Financial Review and asked that this be shared with the members for the Finance & Property Committee. This was agreed. **J Carnegie to progress**

The report was approved.

## **5. Covering Letter (Audit Scotland)**

R Smith talked through the Covering Letter noting that (subject to the finalised annual report and financial statements) it was anticipated that Audit Scotland will issue unqualified audit opinions in the independent auditor's report on 15 December 2020.

## **6. Audit Scotland Annual Report**

R Smith highlighted the Key Messages of the Annual Report as follows:

- The College had to implement a number of changes to its systems of internal control during 2019/20 due to the impact of the cyber-attack and Covid-19. However, high level systems of internal control continued to operate effectively during the year.
- The College has adequate arrangements for the prevention and detection of fraud and other regularities. These include arrangements to prevent fraud and corruption related to procurement activity.
- The College should review its five-year estate strategy to ensure that the existing plans represent the best approach to supporting an excellent, future-focussed curriculum, in a post-Covid world. This should include consideration of the next steps for the Kingsway Tower redevelopment and new build STEM centre.
- The College will play an important role in the delivery of the Tay Cities Region Deal projects by contributing to the objectives of the Skills Investment Plan to boost fair work, inclusive growth and productivity across the region.
- Effective governance and decision-making arrangements were in place during 2019/20 and the College took effective action to adjust its governance arrangements to respond to the challenges presented by Covid-19.
- The College has proper arrangements in place to promote and secure value for money.
- The College reported on a range of positive outcomes from its Good to Great strategy. It also continues to report strong performance against the National Measurement Framework, including student satisfaction results above the national average. As in prior years, the College exceeded its student activity credits target for 2019/20.

R Smith noted his thanks to the College and staff for their assistance during the Audit process especially considering the cyber-attack and Covid-19 pandemic.

The Committee noted the fantastic job done by all involved in such a positive Report The report was approved for submission to the Board. **J Carnegie to progress.**

## 7. Financial Statement for the year ended 31 July 2019

B Ferguson summarised the Financial Statement noting that there were no significant changes since the draft out-turn presented to the Finance & Property Committee in September 2020.

G Robertson congratulated everyone involved for a job well done.

A McCusker noted Audit Scotland's comment re enhancing the Performance Report section of the Financial Statement. R Smith stated that while Audit Scotland recognised the improvements on this area of the report there was still an opportunity to develop this further. The possible inclusion of inf graphics was noted.

The Financial Statement for the year ended 31 July 2020 were approved for submission to the Board of Management meeting on 15 December 2020. **J Carnegie to progress.**

## 8. DATE OF NEXT MEETING

The next Joint Audit and Finance & Property Committee meeting would be confirmed within the 2020/21 Board meetings schedule.

### **Action Point Summary**

<b>Action</b>	<b>Responsibility</b>	<b>Date</b>
Internal audit scope to be shared with Finance & Property Committee members.	J Carnegie	23 December 2020
Submission of external audit report and financial statements to the December Board of Management for approval.	J Carnegie	15 December 2020

**BOARD OF MANAGEMENT**

**Audit & Risk Committee**

**Tuesday 9 March 2020**

---



**Matters Arising**

**PAPER B**

# BOARD OF MANAGEMENT

## Audit & Risk Committee



Tuesday 9 March 2021

### Matters Arising

---

#### *Paper for information*

The following actions were noted from the Tuesday 8 December 2020 Audit & Risk Committee meeting.

Agenda Item No	Action	Current status	Open / Closed
9.0	Update on any additional risk associated with decision not to progress with “Red Forest” technique. <b>J Carnegie</b>	Further explanation on the process/timescales required have been provided in the Internal Audit follow-up report.	Closed

The following actions were noted from the Tuesday 8 December 2020 Joint Audit & Risk and Finance & Property Committee meeting.

Agenda Item No	Action	Current status	Open / Closed
4.0	Internal audit scope to be shared with Finance & Property Committee Members. <b>J Carnegie</b>	Internal Audit Annual Plan is available on the <a href="#">Board Teams</a> site. The internal audit scopes are available from page 123-132 of 133 packaged papers.	Closed
7.0	Submission of external audit report and financial statements to the December Board of Management for approval. <b>J Carnegie</b>	The December Board considered and approved the Audit Scotland Report and Statutory Accounts.	Closed

**Author & Executive Sponsor:** Jaki Carnegie, Vice Principal – Corporate Services

**BOARD OF MANAGEMENT**

**Audit & Risk Committee**

**Tuesday 9 March 2020**

---



**Internal Audit**

**National Fraud Initiative**

**PAPER C**

# Dundee & Angus College

## National Fraud Initiative

dated: 2 March 2021

Final issued: 2 March 2021

LEVEL OF ASSURANCE

Good



# Contents

		Page No.
Section 1	Management Summary	
	• Overall Level of Assurance	1
	• Risk Assessment	1
	• Background	1
	• Scope, Objectives and Overall Findings	1 - 2
	• Audit Approach	3
	• Summary of Main Findings	3
	• Acknowledgements	3
Section 2	Main Findings	4 - 5
Appendix 1	NFI Self-Assessment Checklist	6 - 10

## Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

<b>Good</b>	System meets control objectives.
<b>Satisfactory</b>	System meets control objectives with some weaknesses present.
<b>Requires improvement</b>	System has weaknesses that could prevent it achieving control objectives.
<b>Unacceptable</b>	System cannot meet control objectives.

## Action Grades

<b>Priority 1</b>	Issue subjecting the organisation to material risk and which requires to be brought to the attention of management and the Audit & Risk Committee.
<b>Priority 2</b>	Issue subjecting the organisation to significant risk and which should be addressed by management.
<b>Priority 3</b>	Matters subjecting the organisation to minor risk or which, if addressed, will enhance efficiency and effectiveness.

## Management Summary

### Overall Level of Assurance

Good	System meets control objectives.
------	----------------------------------

### Risk Assessment

This review focused on the controls in place to mitigate the following risk included on Dundee & Angus College's ('the College') Strategic Risk Register:

2.4 – Financial Fraud (risk rating: low).

### Background

As part of the Internal Audit programme at the College for 2020/21 we carried out a review of the College's arrangements for delivering its duties in relation to the National Fraud Initiative (NFI). Our Audit Needs Assessment identified this as an area where risk can arise and Internal Audit can assist in providing assurances to the Principal and the Audit & Risk Committee that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

The NFI is a data-matching exercise led by Audit Scotland to aid the detection of fraudulent payments. NFI allows public bodies to investigate matches and, if fraud or error has taken place, to stop payments and attempt to recover the amounts involved. It also allows auditors to assess the arrangements that bodies have put in place to prevent and detect fraud, including how they approach the NFI exercise itself.

### Scope, Objectives and Overall Findings

The scope of the review did not duplicate the work which Audit Scotland will conduct in order to report on the College's engagement in submitting the base data and investigating any matches identified. Instead, our review focused on the process followed for the 2020/21 NFI exercise, in order to assess lessons learned and progress made since the 2018/19 exercise, where Audit Scotland highlighted issues around the timing of submission of NFI payroll data.

### Scope, Objectives and Overall Findings

The table below notes the objectives for this review and records the results:

Objective	Findings				Action already planned
<b>The objective of this audit was to obtain reasonable assurance that the College can demonstrate:</b>		1	2	3	
1. There are effective arrangements in place to provide the required data, in the format requested, within the timescales set out by Audit Scotland.	Good	0	0	0	✓
2. The Audit & Risk Committee is properly sighted on the work required to ensure compliance with the NFI guidance and is informed of the outcome of the data matching process in order to allow consideration of any associated risks around the prevention and detection of fraud.	Good	0	0	0	
3. The National Fraud Initiative Self-Assessment Checklist has been completed and improvement actions identified	Good	0	0	0	
<b>Overall Level of Assurance</b>	<b>Good</b>	0	0	0	
		System meets control objectives			

### Audit Approach

We reviewed and discussed the College's approach with the senior managers involved in the submission to NFI data match. In addition, we reviewed the approach taken to assess the output from the NFI data match and the actions taken by the College to address any issues identified to ensure any fraud risks were effectively mitigated.

### Summary of Main Findings

#### Strengths

- The College has met the NFI deadlines to upload the required data for the 2020/21 NFI exercise as set by Audit Scotland;
- The College continues to use the NFI website to update the progress of the outcomes of the investigation of the data match outputs;
- At the time of this review the College had completed the investigation of the NFI outputs with no fraudulent activity identified;
- The College's fraud risks are reviewed and updated as an integral part of the Strategic Risk Register process; and
- The Audit & Risk Committee is informed of the progress and outcomes of the NFI exercise and reviews fraud related risk as part of its regular review of the Strategic Risk Register.

#### Opportunities for improvement

- We did not identify any significant weaknesses during our review but noted that the College had already identified opportunities for improvement in the areas of data quality and the completion of Conflict of Interest (Col) declarations. Actions to address these points are being taken forward.

### Acknowledgements

We would like to take this opportunity to thank the staff at the College who helped us during our audit review.



## Main Findings

**Objective 1: There are effective arrangements in place to provide the required data, in the format requested, within the timescales set out by Audit Scotland.**

Our review confirmed that the College did meet the set deadline for uploading the required data for the 2020/21 NFI data match exercise. However, due to the impact of the COVID-19 pandemic and other operational demands, the College was unable to undertake the planned data cleansing exercise prior to the submission of the requested data. While there was a review of the data prior to its submission, the returned data match did identify that 42 of the 205 NFI instances for investigation were data input errors. This represents approximately 20% of the overall number of cases referred by the NFI data match for investigation. However, of these errors, the majority (37) arose from the post cyber-attack period when processing had temporarily changed to manual and extract methodology was not adequately refined.

To ensure data input accuracy for future NFI exercises it is intended that the College will undertake a more detailed review and cleansing of the data prior to its submission for the data matching process.

## National Fraud Initiative

**Objective 2: The Audit & Risk Committee is properly sighted on the work required to ensure compliance with the NFI guidance and is informed of the outcome of the data matching process in order to allow consideration of any associated risks around the prevention and detection of fraud.**

The NFI is regularly discussed at the Audit & Risk Committee through consideration of external and internal audit reports, annual reports, fraud policies etc. Progress with, and outcomes from, the NFI exercise will be submitted to the Audit & Risk Committee at its meeting on 9 March 2021, providing confirmation that the data submission requirements have been met and reporting progress on the cases identified and investigated as part of the data match exercise. At the time of this review the College had completed the investigation of the NFI output with no fraudulent activity identified. One overpayment to a supplier was identified, with the amount recovered.

The output from the NFI data match also identified an issue with the completion of Conflict of Interest (Col) Declarations by Board Members and the College Executive Team as it was noted that voluntary unpaid directorships were not always declared. The investigation did not identify any breach of their Code of Conduct with the incomplete returns. A reminder on the requirements to fully complete this process will be issued to Board and Executive Team members by the Vice Principal People and Performance.

In addition, the Audit & Risk Committee regularly reviews the Strategic Risk Register which includes updates on the fraud risks the College is exposed to.

**Objective 3: The National Fraud Initiative Self-Assessment Checklist has been completed and improvement actions identified.**

The College had not completed the NFI Self-Assessment Checklist. This has been completed as part of our audit (see Appendix 1) and it confirmed that the College had adopted the required steps to successfully complete the NFI exercise. It also identified where further improvements are required and who is taking them forward.

## Appendix 1 – NFI Self-Assessment Checklist

For those charged with governance	Yes/No/Partly	Is action required?	Who by and when?	Comments
<b>Leadership, commitment and communication</b>				
Are we aware of emerging fraud risks, e.g. due to Covid-19, and taken appropriate preventative and detective action?	Yes			Reports are provided to the Audit & Risk Committee, with the next update due at the meeting on 09/03/21. The Strategic Risk Register, including fraud risks is subject to regular updating and review by the Audit & Risk Committee.
Are we committed to NFI? Has the council / board, audit committee and senior management expressed support for the exercise and has this been communicated to relevant staff?	Yes			See above comments.
Is the NFI an integral part of our corporate policies and strategies for preventing and detecting fraud and error?	Partly	Yes	Vice Principal Corporate Services	Yes, the current NFI returns have identified an issue with the completion of Col Declarations by Board Members and the College Executive. A reminder on the requirements to fully complete this process will be issued by the Vice Principal Corporate Services.

## National Fraud Initiative

<b>Leadership, commitment and communication (continued)</b>				
Have we considered using the point of application data matching service offered by the NFI team, to enhance assurances over internal controls and improve our approach to risk management?	No	Yes	Head of Finance – before the next NFI review.	The College is developing its own approach for data cleansing information prior to future submissions. As 20% of the investigations are related to data error matches the aim is to eliminate or significantly reduce this figure.
Are NFI progress and outcomes reported regularly to senior management and elected/board members (e.g. the audit committee or equivalent)?	Yes			See previous comments.
Does internal audit, or equivalent, monitor our approach to NFI and our main outcomes, ensuring that any weaknesses are addressed in relevant cases?	Yes			Internal audit review completed on 2020/21 exercise.
Do we review how frauds and errors arose and use this information to improve our internal controls?	Yes			
Do we publish, as a deterrent, internally and externally the achievements of our fraud investigators (e.g. successful prosecutions)?	Yes			The outcomes and cause of the recent cyber-attack was communicated across the College to heighten awareness of this fraud risk.
<b>Planning and preparation</b>				
Are aware of emerging fraud risks, e.g. due to Covid-19, and taken appropriate preventative and detective action?	Yes			See previous comments on Strategic Risk Register.
Are we investing sufficient resources in the NFI exercise?	Yes			The Key Contact ensured that sufficient resources were available to complete the required task.



## National Fraud Initiative

<b>Planning and preparation (continued)</b>				
Do we plan properly for NFI exercises, both before submitting data and prior to matches becoming available? This includes considering the quality of data.	Partly	Yes	Head of Finance – before the next NFI review.	See previous comments, data cleansing was planned before submitting the data but were unable to undertake due to impact of the COVID-19 pandemic.
Is our NFI Key Contact (KC) the appropriate officer for that role and do they oversee the exercise properly?	Yes			See previous comments.
Do KCs have the time to devote to the exercise and sufficient authority to seek action across the organisation?	Yes			See previous comments.
Where NFI outcomes have been low in the past, do we recognise that this may not be the case the next time, that NFI can deter fraud and that there is value in the assurances that we can take from low outcomes?	No			All output from the NFI review is investigated.
Do we confirm promptly (using the online facility on the secure website) that we have met the fair processing notice requirements?	Yes			Data was submitted in line with set deadlines.
Do we plan to provide all NFI data on time using the secure data file upload facility properly?	Yes			
Have we considered using the point of application data matching service offered by the NFI team to enhance assurances over internal controls and improve our approach to risk management?	No	Yes	Head of Finance – before the next NFI review.	As previously noted, the College is developing its own approach for data cleansing information prior to future submissions.

## National Fraud Initiative

<b>Effective follow up of matches</b>				
Do all departments involved in NFI start the follow-up of matches promptly after they become available?	Yes			The NFI cases for investigation were received on 29/01/21, and these were fully investigated and resolved.
Do we give priority to following up high-risk matches, those that become quickly out-of-date and those that could cause reputational damage if a fraud is not stopped quickly?	Yes			Revised matches were received and reviewed, this process was completed by 6/02/21.
Are we investigating the circumstances of matches adequately before reaching a 'no issue' outcome, in particular?	Yes			Audit review of a sample of matches confirmed that they were satisfactorily investigated and resolved. The issues identified related to Col disclosures and data quality. Resolution of these issues is documented above.
Are we taking appropriate action in cases where fraud is alleged (whether disciplinary action, penalties/cautions or reporting to the Procurator Fiscal)? Are we recovering funds effectively?	Yes			There is a Code of Conduct in place and this will be applied if required following the investigation of the NFI output.
Do we avoid deploying excessive resources on match reports where early work (e.g. on high-risk matches) has not found any fraud or error?	Yes			All data match outputs were investigated and resolved.
Where the number of high-risk matches is very low, are we adequately considering the medium and low-risk matches before we cease our follow-up work?	N/A			All data match outputs were assessed as high-risk, therefore were all investigated and resolved.
Overall, are we deploying appropriate resources on managing the NFI exercise?	Yes			See previous comments, to date all NFI deadlines have been met.

## National Fraud Initiative

Recording and reporting				
Are we recording outcomes properly in the /secure website and keeping it up-to-date?	Yes			
Do staff use the online training modules and guidance on the secure website, and do they consult the NFI team if they are unsure about how to record outcomes (to be encouraged)?	Yes			The Key Contact is experienced in the undertaking of the NFI process.
If, out of preference, we record some or all outcomes outside the secure website, have we made arrangements to inform the NFI team about these outcomes?	N/A			The website is used to update all elements of the NFI process.

#### **Aberdeen**

45 Queen's Road  
Aberdeen  
AB15 4ZN

T: 01224 322100

#### **Dundee**

The Vision Building  
20 Greenmarket  
Dundee  
DD1 4QB

T: 01382 200055

#### **Edinburgh**

Ground Floor  
11-15 Thistle Street  
Edinburgh  
EH2 1DF

T: 0131 226 0200

#### **Glasgow**

100 West George Street  
Glasgow  
G2 1PP

T: 0141 471 9870

MHA Henderson Loggie is a trading name of Henderson Loggie LLP, which is a limited liability partnership registered in Scotland with registered number SO301630 and is a member of MHA, an independent member of Baker Tilly International Ltd, the members of which are separate and independent legal entities

© 2019 MHA Henderson Loggie

 **mha**  
HENDERSON LOGGIE

[hlca.co.uk](http://hlca.co.uk) | [info@hlca.co.uk](mailto:info@hlca.co.uk)

**BOARD OF MANAGEMENT**

**Audit & Risk Committee**

**Tuesday 9 March 2020**

---



**Internal Audit**

**Software Development / Implementation**

**PAPER D**

# Dundee & Angus College

## Systems Development / Implementation

Completed: 28 February 2021

Final issued: 1 March 2021

LEVEL OF ASSURANCE

Good

# Contents

		Page No.
Section 1	Management Summary	
	• Overall Level of Assurance	1
	• Risk Assessment	1
	• Background	1
	• Scope, Objectives and Overall Findings	2
	• Audit Approach	2
	• Summary of Main Findings	2 - 3
	• Acknowledgements	3
Section 2	Main Findings	4 - 8

## Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

## Action Grades

Priority 1	Issue subjecting the organisation to material risk and which requires to be brought to the attention of management and the Audit & Risk Committee.
Priority 2	Issue subjecting the organisation to significant risk and which should be addressed by management.
Priority 3	Matters subjecting the organisation to minor risk or which, if addressed, will enhance efficiency and effectiveness.

## Management Summary

### Overall Level of Assurance

Good	System meets control objectives.
------	----------------------------------

### Risk Assessment

This review focused on the controls in place to mitigate the following risks included on Dundee & Angus College's ('the College') Strategic Risk Register:

- 3.8 – Breach of data security / data protection (risk rating: low);
- 4.3 – Breach of ICT / Cyber security (risk rating: low); and
- 4.4 – ICT infrastructure fails to support effective data security / data protection (risk rating: low).

### Background

As part of the Internal Audit programme at the College for 2020/21 we carried out a review of the progress that the College has made in improving its cyber resilience following the cyber-attack in January 2020 which caused significant disruption to College operations, together with a review of IT controls in place specifically relating to home working. Our Audit Needs Assessment identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Principal and the Audit & Risk Committee that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

In the wake of the Wannacry ransomware attacks in May 2017, the Scottish Government published its Public Sector Action Plan on Cyber Resilience, outlining a common, effective, risk-based approach to cyber-security across the public sector. In line with the requirements of the Scottish Government's action plan, the College attained Cyber Essentials Plus accreditation in December 2019, assuring that the College has in place five critical controls to reduce vulnerability to the most common internet-based threats (including hacking and phishing).

The College does not formally record all attempted cyber-attacks, unless these are extraordinary or significant in some way, due to the daily volume of attacks. Attempted cyber-attacks are treated as 'business as usual', as each day the College's firewall (in common with other large public bodies) blocks a high volume of attempted phishing and spoofing emails (the attempt to procure or alter staff personal data through fraud and social engineering); and other unsuccessful external attempts to penetrate the College's firewall (for the purposes of hacking; or transmission of malware, viruses, trojan horses, and ransomware). The College's Networks team 'patch' identified security vulnerabilities on a rolling basis to minimise risk. The College has in place the following five key security controls and received externally validated Cyber Essentials Plus accreditation accordingly: Firewalls; Secure Configuration; User Access Control; Malware Protection; and Patch Management.



### Scope, Objectives and Overall Findings

Remote working due to the COVID-19 pandemic heightens existing cyber risks and introduces new ones to many organisations. This audit considered whether the internal control environment is sufficiently robust to protect the College.

The table below notes the objectives for this review and records the results:

Objective	Findings				Actions already in progress
The objectives of this audit were to obtain reasonable assurance that:		1	2	3	
1. appropriate progress is being made to implement the recommendations from the cyber-attack.	Good	0	0	0	✓
2. remote desktop and remote applications controls are in place.	Good	0	0	0	
3. controls have been implemented to ensure that electronic and digital communication tools, including email, Zoom and Microsoft Teams, are secure.	Good	0	0	0	
Overall Level of Assurance	Good	0	0	0	
System meets control objectives					

### Audit Approach

From discussion with the Head of ICT and other members of the ICT team, and review of relevant policies, procedures, and guidance, we identified the key internal controls in place and compared these with expected controls for cyber security published by the National Cyber Security Centre. We have reported on any areas where expected controls were found to be absent or where controls could be further strengthened.

### Summary of Main Findings

#### Strengths

- Following the forensic review into the circumstances of the cyber-attack in 2020 the College acted swiftly to address the key findings with seven of the eight recommendations implemented immediately. The College remains on track to implement the remaining action by the July 2021 target date. We also noted that the College has implemented further measures over and above the recommendations made following the cyber-attack report which are designed to reduce the impact of future cyber-attacks.
- Good progress has been made in implementing the recommendations relating to information and cyber security controls raised in Internal Audit report 2020/03 – IT Network Arrangements / IT Strategy, issued in April 2020, with four of the five recommendations now fully implemented.

### Summary of Main Findings (continued)

#### Strengths (continued)

- Following a substantial review of information and cyber security services conducted by Higher Education / Further Education Shared Technology and Information Services (HEFESTIS), the College has implemented a framework for Information and Cyber Security (ICS) risk management. The HEFESTIS review observed that there had been a significant and substantial improvement on the recorded College ICS risk posture over the period January to October 2020.
- Our review identified several good practice controls in place to support remote working for users whilst making the infrastructure secure.
- Microsoft Teams has now become a primary operational and communication tool for the College. Sign-in for users to Microsoft Teams is enabled using their College email address and their College access credentials which allows the ICT team full control over who can access the service. The College has also integrated Microsoft Teams with Azure Active Directory which allows for improved security and configuration. A range of security features are built into Microsoft Teams including, multi-factor authentication (MFA) access controls, enforced least privileged access rights across Microsoft Teams and Office 365, classification criteria for sensitive data, prevention of file downloads to devices not approved or managed by the College, and the ability to audit and trace data sharing with external users.
- Following a risk assessment of Zoom, together with the findings of the forensic review following the cyber-attack, the College has taken the decision not to allow the use of Zoom by staff.
- The implementation of Office 365 and the associated controls which have been enabled has improved the security of the College email system, which is a common attack vector through social engineering, malware, or phishing attacks.

#### Weaknesses

- No significant weaknesses were identified during our review.

### Acknowledgements

We would like to take this opportunity to thank the staff at the College who helped us during our audit.



## Main Findings

### **Objective 1: Appropriate progress is being made to implement the recommendations from the cyber-attack.**

Following the cyber-attack in January 2020 a detailed forensic investigation was conducted by the College's ICT team, supported by the JANET Computer Security Incident Response Team (CSIRT) and the North Regional Chief Information Security Officer (CISO) from the Higher Education / Further Education Shared Technology and Information Services (HEFESTIS). In March 2020, the College's Head of ICT reported to the Board the circumstances which led to the cyber-attack and identified eight improvement actions to strengthen the College's cyber-security environment. We noted that the findings from the review identified the factors that allowed the specific type of cyber-attack to be successful and to reduce the risk of recurrence of that type of cyber-attack, or similar. Seven of the eight recommendations were implemented immediately. During this review we discussed progress made with the remaining recommendation with the Head of ICT and noted that the College is exploring software solutions which will further limit the types of scripts that are able to run across networked services and improve the event logging and alerting procedure to allow the ICT team to proactively respond to threats. The College remains on track to implement the remaining action by the July 2021 target date. We noted one further action which, although had previously been implemented, the College is now looking at alternative options to further strengthen network architectural controls.

In January 2020, prior to the cyber-attack, an internal audit review had commenced looking at the College's cyber security position measured against guidance issued by the National Cyber Security Centre (NCSC). The findings from the review were published in internal audit report, 2020/03 – IT Network Arrangements / IT Strategy, issued in April 2020, which highlighted five recommendations relating to cyber-security governance and controls. The Vice Principal, Corporate Services reported progress made on those recommendations to the Audit & Risk Committee (ARC) in September and December 2020. We noted from review of the ARC papers and through discussion with the Head of ICT that four of the five recommendations have now been implemented, including:

- inclusion of cyber security on the strategic risk register and development of a Cyber Security Strategy;
- provision of remote and digital learning programmes to staff and continued assessments of staff information security skills requirements;
- development of a cyber incident response plan; and
- technical changes made to devices to enable encryption of USB devices.

## Systems Development / Implementation

### Objective 1: Appropriate progress is being made to implement the recommendations from the cyber-attack (continued).

The remaining recommendation, related to developing a programme of information and cyber security training, is currently in progress with mandatory training developed and issued to all staff. Checks will be made during March 2021 to review completion rates and follow-up with staff that have yet to complete. A cyber security training and evaluation exercise has also been scheduled for March 2021. Progress made with the previously raised internal audit recommendations will be formally reported as part of the internal audit Follow-up review later in 2021.

HEFESTIS is a non-profit consulting agency working exclusively with partners in the Higher and Further education sector in Scotland. HEFESTIS provides a shared CISO and information security service to the College. Over the course of 2019 and 2020 HEFESTIS worked with the College to improve the quality and effectiveness of risk management and security maturity services. In November 2020 HEFESTIS reported the findings of its review of the College's Information and Cyber Security (ICS) Risk Actions Issues and Decisions (RAID) log including ongoing information and cyber security management activity over the period of January to October 2020.

Following a substantial review of information and cyber security services conducted for the College over early 2020, a framework for ICS risk management was introduced. The purpose of the review was to articulate and put in place measures to improve the cyber security risk posture of the College. HEFESTIS concluded in its review that:

- there had been a significant and substantial improvement on the recorded College ICS risk posture over the reporting period;
- improved information risk governance structures had been established and risk mitigation activity had been applied to all recorded categories of greatest ICS risk via those structures;
- areas of greatest improvement included implementation of multi-factor authentication (MFA), improved operational efficiency and introduction of ICS risk management procedures;
- progress in policy development, governance, incident management and network security had also contributed to a hardening of the ICS maturity posture; and
- although there was a significant increase in external risk and threat level due to COVID-19 related change, such as the rapid deployment of home working capability and related digital tools, and heightened threat actor activity, there was no negative impact on the College's ICS management controls or overall cyber security posture.

Three recommendations were raised in the HEFESTIS report relating to: further supporting and developing the ICS governance structures, which had been established as part of the ICS risk management framework; implementing the suite of KPIs identified by HEFESTIS to measure and monitor risk and security activity; and continue to implement the actions included in the Public Sector Action Plan, Cyber Resilience Action Plan and to maintain Cyber Essentials Plus certification. Discussion with the Head of ICT noted that work continues to be made on all three areas highlighted by HEFESTIS and progress updates will be reported to the College groups that form part of the information risk management governance structure.

## Systems Development / Implementation

### **Objective 1: Appropriate progress is being made to implement the recommendations from the cyber-attack (continued).**

We also noted that the College has implemented further measures over and above the recommendations raised in the cyber-attack, internal audit, and HEFESTIS reports referred to above, which would reduce the impact of future cyber-attacks including:

- cloud authentication for users accessing College services;
- the cyber-attack encrypted files on the College domains and so the College has blocked the use of file shares and instead staff now use OneDrive and Microsoft Teams for sharing and storing documents;
- reduction of the attack surface by removal of legacy domains and moving more services to the cloud; and
- reduction of potential attack vectors through encryption of all mobile devices and removal of legacy email addresses and domains.

Overall, we have concluded that positive progress has been made by the College since the cyber-attack to strengthen and update cyber controls and cyber resilience.



### Objective 2: Remote desktop and remote applications controls are in place.

With the increased use of cloud technologies and number of users working remotely the challenge for the College is to strike a balance between ensuring seamless access to services and applications whilst maintaining the security of critical infrastructure. To support remote working for users whilst making the infrastructure secure we noted that the following good practice controls are in place:

- most users connect to the College network and services using a College owned and managed device. Where users connect using personal devices additional controls have been put in place as highlighted below;
- all managed devices are encrypted;
- antivirus protection is installed with local and network firewalls in place;
- network traffic is filtered to process the flow of legitimate traffic and block potential intruders looking to exploit the network. Filtering allows the College to analyse and prevent inbound requests that come from unauthorised IP addresses, as these are inherent risks to the system. Configuration blocking incoming requests from unknown sources is set within the firewall inbound rules;
- operating systems and other software are regularly updated and patched;
- strong password policy, automatic login disabled, and automatic lock enabled;
- mobile device management software in use which allows managed devices to be located and wiped in the event of loss or theft;
- where the College has not been able to use managed devices, users have been provided with information security guidance that explains the security measures required and recommended for remote workers;
- security awareness training has been provided to users;
- to ensure network security the College uses Virtual Private Network (VPN) to secure access to the corporate network. As remote users might connect from external untrusted networks, network protocols are used for application security;
- Two-Factor Authentication in place to protect VPN accounts and cloud services from unauthorised access;
- default port numbers not used when setting up remote connections; and
- security policy implemented for third parties working on the network.

Although the above measures improve the security of the College IT, the potential attack surface has increased due to the number of home networks now in scope. To mitigate the additional risk, we noted several best practices have been put in place to further improve risk management:

- basic housekeeping practices for user account management, covering deletion / disablement of stale and unused user accounts, group profiles for assigning user access rights with least privileged protocols followed, and removal of unused network services;
- an account lockout policy in place to prevent attackers from getting access to the College internal network by guessing a user's password; and
- Active Directory and Azure AD groups for access control across the infrastructure. Regular review of groups and group membership to make sure no one has excessive permissions.

## Systems Development / Implementation

**Objective 3: Controls have been implemented to ensure that electronic and digital communication tools, including email, Zoom and Microsoft Teams, are secure.**

Prior to the Covid-19 pandemic, the College had commenced implementation of Microsoft Teams as part of its Digital Strategy and to create a digital environment with cloud hosted services at the forefront. The implementation of cloud services such as Office 365, OneFile and Microsoft Teams prior to January 2020 also helped to minimise the impact of the cyber-attack which affected the College's server environment. The national lockdown and the move to working from home led to the College deploying the use of Microsoft Teams at pace during the early phase of the pandemic and it has now become a primary operational and communication tool.

Microsoft Teams is a collaborative workspace within Microsoft 365 / Office 365 that acts as a central hub for workplace conversations, collaborative teamwork, video chats and document sharing. Sign-in for users to Microsoft Teams is enabled using their College email address and their College access credentials which allows the ICT team full control over who can access the service. The College has also integrated Microsoft Teams with Azure Active Directory which allows for improved security and configuration. A range of security features are built into Microsoft Teams including, MFA access controls, enforced least privileged access rights across Microsoft Teams and Office 365, classification criteria for sensitive data, prevention of file downloads to devices not approved or managed by the College, and the ability to audit and trace data sharing with external users.

Following a risk assessment of Zoom, together with the findings of the forensic review following the cyber-attack, the College took the decision early in the pandemic to implement a policy to prevent the use of Zoom by staff for internal meetings. Network access and application controls ensure that the client version of Zoom, and other similar platforms, cannot be installed on College managed devices. Zoom can be accessed through a web browser with no need to link user access to the College domain and / or Office 365 accounts, which reduces the level of control which the College has over security configurations. However, Zoom is still permitted for use by staff for meetings with external parties.

The implementation of Office 365 has also improved the security of the College email system, which is a common attack vector through social engineering, malware, or phishing attacks. This includes:

- Advanced Threat Protection is in place which helps by stopping malicious links and attachments before they get to a user's email inbox. It opens the attachments and links in a virtual environment, separate from the College environment, and checks for malicious activity before the email gets to the inbox;
- Emails are encrypted; and
- Data Loss Prevention (DLP) ensures sensitive information does not get sent outside of the College to begin with and applies to more than just email as it also includes SharePoint, OneDrive and Office programs like Excel and Word. DLP policies monitor the College environment for sensitive data and prevents users from sending that information externally.

#### **Aberdeen**

45 Queen's Road  
Aberdeen  
AB15 4ZN

T: 01224 322100

#### **Dundee**

The Vision Building  
20 Greenmarket  
Dundee  
DD1 4QB

T: 01382 200055

#### **Edinburgh**

Ground Floor  
11-15 Thistle Street  
Edinburgh  
EH2 1DF

T: 0131 226 0200

#### **Glasgow**

100 West George Street  
Glasgow  
G2 1PP

T: 0141 471 9870

MHA Henderson Loggie is a trading name of Henderson Loggie LLP, which is a limited liability partnership registered in Scotland with registered number SO301630 and is a member of MHA, an independent member of Baker Tilly International Ltd, the members of which are separate and independent legal entities

© 2019 MHA Henderson Loggie

 **mha**  
HENDERSON LOGGIE

[hlca.co.uk](http://hlca.co.uk) | [info@hlca.co.uk](mailto:info@hlca.co.uk)



**BOARD OF MANAGEMENT**

**Audit & Risk Committee**

**Tuesday 9 March 2020**

---



**Internal Audit**

**20/21 Progress Report**

**PAPER E**

# Dundee & Angus Council

## Internal Audit Programme Report 2020/21 Annual Plan

9 March 2021

Now, for tomorrow

# Internal Audit Progress Report

## March 2021

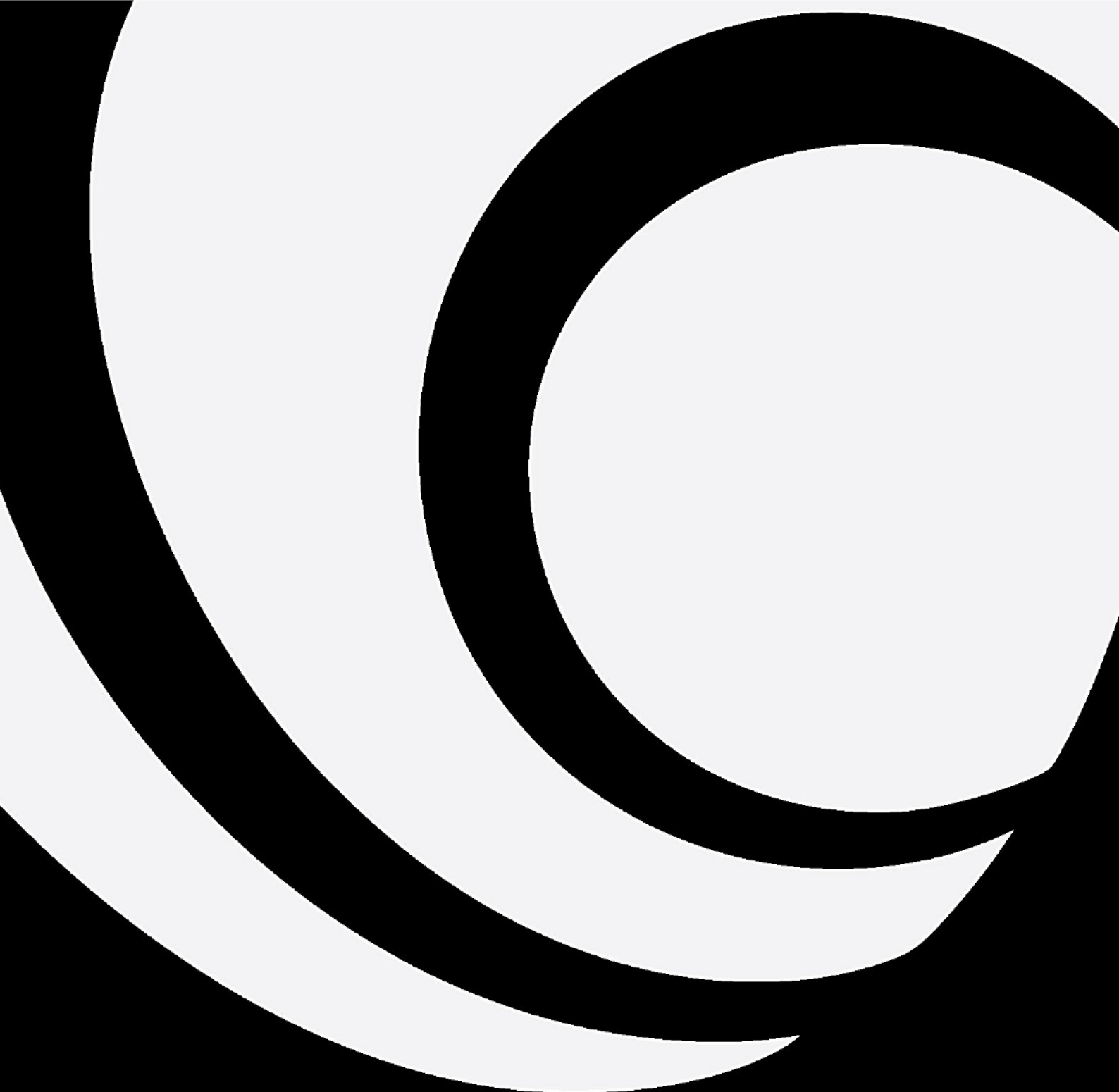
Progress made in delivering the annual plan for 2020/21, approved in September 2020, is shown below.

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit and Risk Committee	Comments
Annual Plan 2020/21	September 2020	Draft 24/07/20 2 <sup>nd</sup> Draft 07/09/20 Final 22/09/20	2021/01	N/A	22/09/20	
Health, Safety and Wellbeing	September 2020	Draft 11/09/20 Final 14/09/20	2021/02	Good	22/09/20	
Budgetary Control (financial reporting)	May 2021					Fieldwork agreed for w/c 01/03/21
National Fraud Initiative	March 2021	Draft 02/03/21 Final 02/03/21	2021/04	Good	09/03/21	
Economic Recovery	May 2021					Fieldwork proposed for w/c 29/03/21
Systems Development / Implementation	March 2021	Draft 28/02/21 Final 01/03/21	2021/03	Good	09/03/21	
Follow Up Reviews	September 2021					Fieldwork proposed for w/c 26/07/21

Audit Area	Planned reporting date	Report status	Report Number	Overall Conclusion	Audit and Risk Committee	Comments
Credits audit	November 2021					Fieldwork proposed for w/c 30/08/21
Bursary, childcare and hardship funds	November 2021					Fieldwork proposed for w/c 06/09/21
EMA audit	November 2021					Fieldwork proposed for w/c 06/09/21

Gradings are defined as follows:

<b>Good</b>	System meets control objectives.
<b>Satisfactory</b>	System meets control objectives with some weaknesses present.
<b>Requires improvement</b>	System has weaknesses that could prevent it achieving control objectives.
<b>Unacceptable</b>	System cannot meet control objectives.

**Aberdeen**

45 Queen's Road  
Aberdeen  
AB15 4ZN

T: 01224 322100

**Dundee**

The Vision Building  
20 Greenmarket  
Dundee  
DD1 4QB

T: 01382 200055

**Edinburgh**

Ground Floor  
11-15 Thistle Street  
Edinburgh  
EH2 1DF

T: 0131 226 0200

**Glasgow**

100 West George Street  
Glasgow  
G2 1PP

T: 0141 471 9870

MHA Henderson Loggie is a trading name of Henderson Loggie LLP, which is a limited liability partnership registered in Scotland with registered number SO301630 and is a member of MHA, an independent member of Baker Tilly International Ltd, the members of which are separate and independent legal entities

© 2019 MHA Henderson Loggie

**BOARD OF MANAGEMENT**

**Audit & Risk Committee**

**Tuesday 9 March 2020**

---



**Internal Audit**

**Follow-Up Summary**

**PAPER F**

# BOARD OF MANAGEMENT



## Audit & Risk Committee

Tuesday 9 March 2021

### Internal Audit Outstanding Actions Follow-up Summary

#### *Paper for information*

#### 1. Introduction

This report provides an update on the Internal Audit actions that are not yet closed off. These are a combination of actions:

- that are not yet due to be completed or;
- where the originally anticipated deadline has passed or;
- that are partially completed.

The report also includes other related updates.

#### 2. Recommendations

Members are asked to note the progress highlighted in Appendix 1 and 2.

#### 3. Background

The following provides a summary of the progress of actions since the September 2020 meeting.

		Number of Actions Outstanding (& Priority Grades)		
Audit Area	Report Grades	1	2	3
Student Engagement/Students' Association	Good	-	-	1
HR / Payroll	Good	-	-	1
Procurement and Creditors/ Purchasing	Good	-	-	1
IT Network Arrangement / IT Strategy	Satisfactory	-	-	1 1
Student Activity Date	n/a		1	2
Total		-	1	7



Complete or on target to complete

Behind schedule by < 3 months from original deadline

Behind schedule by > 3 months, or in danger of not being delivered

Of the 8 outstanding actions, since the last Audit & Risk Committee, good progress has been made:

- 5 are Complete
- 3 are behind schedule >3 months

The outstanding actions with the respective progress updates are detailed in the

appendix below.

#### **4. Cyber Incident**


The following provides a summary of the progress on the recommendations from the Cyber Incident that affected the college in January 2020. You will notice a further internal audit has been completed over the last month that also reviews progress of recommendations following the incident. HEFESTIS are also reporting to the Committee at this meeting on progress being made.

Due to the sensitivity of the report the progress will be reported as a separate Appendix.

The report should continue to be treated as sensitive and confidential and not be shared wider.

Of the remaining 2 (of 12) outstanding recommendations since the report in November 2020 the update remains the same:

- one is paused and has moved into options appraisal stage
- an alternative is being progressed for one

 Complete or on target to complete within original deadline

#### **5. Catering Business Process Review Update**

At the November 2019 Audit & Risk Committee it was agreed that a regular update on progress of the Catering Business Process Review would be welcomed. A series of workstreams are in place, however as reported to the May/September/December meetings there is an ongoing requirement for physical distancing. The catering function has only reopened to deliver food to the Arbroath nursery and will only deliver limited food to those curriculum areas where return to campus has been deemed critical. It is unlikely that there will be any reopening of the catering areas until after the Easter break and even then it will likely remain as a limited service.

#### **6. Fraud Initiative Update**

Our second biannual (every 2 years) data-matching exercise has taken place. The findings of this data matching exercise are provided at Appendix 3 below. It is pleasing that all investigation work on the matches are closed off with no frauds identified. There was one error which was corrected.

The Internal Audit on the National Fraud Initiative was scheduled with the aim of coinciding with the matches becoming available. We are pleased that this report provided us with a “Good” level of assurance.

There have been no further workshops on the delivery of the revised Fraud, Bribery and Corruption policy. These will be scheduled for later in the year.

#### **7. Link to Strategic Risk Register**

Consideration of the outstanding actions is intended to provide Members with reassurance that actions for improvement are being progressed and addressed.



Progressing these Internal Audit outstanding actions will support the mitigation of a range of risks identified within the Strategic Risk Register namely;

2.2 – failure to achieve institutional sustainability

2.4 – financial fraud

3.1 – failure to reach aspirational standards in learning, teaching and service delivery

3.2 – failure to achieve/maintain compliance arrangements

3.3 – serious accident, incident or civil/criminal breach, legal action

3.4 – loss of reputation with key stakeholders

3.7 – breach of data security/data protection

3.8 – failure to meet Prevent and related obligations

3.8 – arrangements do not minimise risk associated with Modern Slavery

4.4 – failure to support effective data security/data protection

**Author & Executive Sponsor:** Jaki Carnegie, Vice Principal – Corporate Services

## Outstanding Action Update

Appendix 1

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at March 2021)
2019/07	R1 - Student Engagement / Students' Association	3	Satisfactory	A formal Learner Engagement Strategy should be developed which contains aims and objectives which are clearly linked to the College's Regional Outcome Agreement and to the College's partnership agreement with the Students' Association; identifies and priorities learner engagement activity; and identifies actions which focus specifically on how the Strategy will be implemented in practice.	Learner Engagement Manager	<del>Jun-20</del> <del>Dec-20</del> Aug-21	<u>Behind Schedule</u> Draft strategy document developed in line with original timescale by LE Manager for final discussion/approval.  As was reported and accepted at December's Committee meeting this has not been progressed at the current time due to Covid-19 adaptations in working arrangements / approaches. It is not felt to be appropriate to finalise this until 'post Covid-19' learning and study arrangements are clearer.
2020/03	R2 - Network Arrangements / IT Strategy	3	Satisfactory	Develop a programme of information and cyber security training for staff and students to mitigate information security risks, covering: <ul style="list-style-type: none"> <li>the College's Information Security Strategy and associated IT security</li> </ul>	Head of ICT	Jan-21	<u>Complete</u> Rolled out to all staff

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at March 2021)
				<p>policies;</p> <ul style="list-style-type: none"> <li>cyber security risks and strategies for defence, covering internet safety, mobile and home working, phishing, and prevention against malware.</li> <li>an induction process for new staff (and where applicable contractors and third-party users);</li> <li>regular refresher training on the security risks to the College;</li> <li>supporting staff in information security roles to enrol on a recognised certification scheme;</li> <li>monitoring the effectiveness of security training; and</li> <li>promoting an incident reporting culture.</li> </ul>			
2020/03	R3 - Network Arrangements / IT Strategy	3	Satisfactory	Once training has been delivered (see R2) mechanisms should be developed and implemented to test the effectiveness and value of the security training provided to staff and students. This should be delivered	Learning & Digital Resource Manager	Jun-20 Jun-21	<u>Behind Schedule</u> Revised Digital Skills Capability Assessment is currently being developed. This will be included in the Learn@D&A Induction and also form part of the new suite of Getting Ready for College courses that will be

Year	Audit Area Report Title	Priority Action Grade	Report Grade	Action	Responsible Officer	Deadline	Progress (as at March 2021)
				<u>through</u> formal analysis of the section on information security within the Digital Skills Capability Assessment. Those areas of the College which routinely feature in security reports (or achieve the lowest feedback from information security questionnaires) should be targeted and prioritised for further training.			offered to new students. A staff version is also being developed, again this will be included in the staff induction process and offered out to staff on an agreed development cycle.
2020/04	R1 – Payroll & HR	3	Good	The Payroll Procedural Notes should be updated to provide a comprehensive guide for any member of staff brought in to cover for the Payroll Officer or Payroll Assistant	Head of Finance	<del>Aug-20</del> <del>Dec-20</del> March 21	<u>Behind Schedule</u> Commenced and on schedule to complete this quarter.
2020/05	R1 – Procurement & Creditors / Purchasing	3	Good	The next iteration of the procurement strategy and the procurement policy should make specific reference to the ways in which risks around modern slavery will be dealt with through the procurement arrangements.	Head of Finance / Procurement Manager	<del>Nov-20</del> March 21	<u>Complete</u> Policy drafted for approval by the Finance & Property Committee schedule to meet on 2 March 2021
2020/07	R1 – Student Activity Data	3		Review course superclass codes to ensure they best describe the academic subject areas.	Data Management Team Leader	Jun-21	<u>Complete</u> Superclass codes reviewed and final checks will be undertaken before submission of final FES.

<b>Year</b>	<b>Audit Area Report Title</b>	<b>Priority Action Grade</b>	<b>Report Grade</b>	<b>Action</b>	<b>Responsible Officer</b>	<b>Deadline</b>	<b>Progress</b> (as at March 2021)
2020/07	R2 – Student Activity Data	2		The College should ensure that a schedule of milestones agreed at enrolment is maintained for all distance learning programmes. This should include a record of the estimated amount of time that students are expected to take to complete each element of the course, to evidence eligibility of the Credit values claimed	Head of Administrative Operations	Jun-21	<u>Complete</u> All remote learning packages now have milestone / participation activities and this is used to evidence credit claims and participation.
2020/07	R3 - Student Activity Data	3		The College should ensure evidence of progression and participation / engagement is retained to evidence eligibility of the Credits claimed for distance / work-based learning students. Where curriculum staff identify that no evidence is available or that students are no longer engaging this should be notified to the Student Records team to ensure that the Credits are removed from the Credit claim.	Data Management Team Leader	Jun-21	<u>Complete</u> All remote and distance learning packages now have engagement and participation monitoring and evidence is available to support the credit claim.

**SENSITIVE AND CONFIDENTIAL: NOT TO BE SHARED WIDER**

Recommendation	Technical Detail/Progress Update	Deadline	Progress (as at March 2021)
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

Recommendation	Technical Detail/Progress Update	Deadline	Progress (as at March 2021)
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Recommendation	Technical Detail/Progress Update	Deadline	Progress (as at March 2021)
	<div data-bbox="667 225 2085 304" data-label="Text"> <p>[REDACTED]</p> </div> <div data-bbox="667 341 2074 730" data-label="Text"> <p>[REDACTED]</p> </div>		

## National Fraud Initiative - Data Matches 2020

<b>Report Name</b>	<b>Total All</b>	<b>Status</b>	<b>Processed</b>	<b>Frauds</b>	<b>Errors</b>
Payroll to Payroll, high quality	6	Closed	6	0	0
Payroll to Payroll, same phone	2	Closed	2	0	0
Payroll to Creditors	2	Closed	2	0	0
Payroll to Creditors	1	Closed	1	0	0
Duplicate creditors by creditor name	1	Closed	1	0	0
Duplicate creditors by bank account	1	Closed	1	0	0
Duplicate records by invoice amount	121	Closed	121	0	1
VAT overpaid	57	Closed	57	0	0
Duplicate records by supplier invoice, different creditor ref and name	5	Closed	5	0	1
Duplicate records by postcode, reference and supplier invoice number and invoice date	1	Closed	1	0	0
Procurement - Payroll to Companies House (Directors)	5	Closed	5	0	0
Procurement - Payroll to Companies House (Directors)	3	Closed	3	0	0
	<b>205</b>		<b>205</b>	<b>0</b>	<b>2</b>

<b>Closed/ No Issue</b>	<b>Data Extract error</b>	<b>2018 duplicate</b>	<b>Satisfactorily explained</b>	<b>Already corrected</b>
6			6	
2			2	
2			2	
1			1	
1		1		
1			1	
121		4	116	1
57	42	13	2	
5		4		1
1			1	
5			5	
3			3	
<b>205</b>	<b>42</b>	<b>22</b>	<b>139</b>	<b>2</b>



**BOARD OF MANAGEMENT**

**Audit & Risk Committee**

**Tuesday 9 March 2020**

---



**Strategic Risk & COVID Register**

**9.1 Strategic Risk Register**

**PAPER G**

**9.2 COVID Risk Register**

**PAPER H**

## **Strategic Risk Register Update**

---

### ***Paper for approval***

#### **1. Strategic and COVID Risk Registers**

A copy of the March 2021 draft Strategic Risk Register and COVID 19 Risk Register are enclosed. No changes have been made to the full Strategic Risk Register since the previous meeting, but two changes have been made to the COVID 19 Risk Register since this was last approved as noted below. These changes were discussed and agreed at the Learning, Teaching and Quality Committee meeting on 10 February 2020.

- 3.1 Failure to reach aspirational standards in learning, teaching and service delivery

Following on from the most recent announcements in respect of COVID restrictions for practical subject areas the likelihood of impact on risk 3.1 has been increased, moving this from green to amber.

- 3.5 Reputational Risk – Loss of reputation with key stakeholders

A change in risk likelihood has been made to risk 3.5 in relation to possible impact on our reputation with stakeholders (especially schools, parents and employers) due to the disproportionate impact of current COVID restrictions on senior phase and apprenticeship groups compared with those studying through schools and private training providers.

#### **2. Brexit Risk**

Whilst no change has been made to the Strategic Risk Register, members of the Committee may wish to note that review is continuing in respect of the impact of the UK leaving the EU. This work is supported by on-going input from the Scottish Funding Council who maintain a 'live' summary of key Brexit related issues and impacts.

### **3. Scenario Planning**

Whilst no change has been made to the Strategic or COVID Risk Registers, members of the Committee should note that extensive work has been developed by the College to support and inform sector wide scenario planning in respect of the likelihood and quantity of student deferrals into academic year 2021/22 (and potentially 2022/23) as a result of the pandemic. This work has been discussed in COVID updates to each Board Committee and used to inform national contingency planning through the Learner Journey Taskforce.

### **4. Approvals**

In respect of the above information approval for the following actions is sought.

- Approval of the Strategic and additional COVID Risk Registers

**Author and Executive Sponsor:** Steve Taylor, Vice Principal People and Performance



# STRATEGIC RISK REGISTER

**2020 - 2021**

As at March 2021

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
1	Strategic and Structural									
1.1 LT&Q	Failure of College strategy to meet the needs of the D&A Region and/or national priorities (eg Employability, DYW, attainment, articulation)	4	4	16	<ul style="list-style-type: none"><li>Robust strategic planning</li><li>Effective environmental scanning</li><li>Strong partnerships</li><li>Clear links between strategy and practice</li><li>Concerted demands for increased activity levels</li></ul>	4	1	4	<ul style="list-style-type: none"><li>Robust monitoring via ROA</li><li>Clear performance metrics</li><li>Amendment of strategic direction/ plans</li><li>Rolling curriculum review</li></ul>	Prin & Chair
1.2 Board	College may be disadvantaged by changes to either UK or Scottish Government policies	4	3	12	<ul style="list-style-type: none"><li>Effective environmental scanning</li><li>Negotiation/influence at national level</li></ul>	4	2	8	<ul style="list-style-type: none"><li>Review of changes and amendment of strategic direction/plans</li><li>Financial strategy sensitivities</li></ul>	Prin & Chair
1.3 Board	College disadvantaged by changes arising from UK leaving European Union	5	4	20	<ul style="list-style-type: none"><li>Negotiation/influence at national level</li><li>Review of activities/ projects</li><li>Responsiveness to new opportunities</li></ul>	5	3	15	<ul style="list-style-type: none"><li>Review of changes and amendment of strategic direction/plans/ curriculum</li><li>Financial strategy ESF sensitivity</li><li>Workforce planning</li><li>International strategy &amp; planning</li><li>Brexit planning</li></ul>	Prin

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

Post Holders	ELT	Executive Leadership Team	Prin	Principal	Score	Impact	Likelihood
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
<b>1</b>	<b>Strategic and Structural</b>									
<b>1.4 Board</b>	<p>Difficulties or over commitment arising within large scale/national College led initiatives or projects impact negatively on:</p> <ul style="list-style-type: none"> <li>Ability of the College to meet key regional strategies/objectives</li> <li>Financial loss or unmanageable financial risk</li> <li>Reputational loss</li> </ul>	4	3	12	<ul style="list-style-type: none"> <li>Effective project/activity management in place</li> <li>Clear governance structures</li> <li>Project/initiative finances clearly incorporated within College financial strategy and plans</li> <li>End of project and exit/contingency planning</li> </ul>	3	2	6	<ul style="list-style-type: none"> <li>Regular project updates at Executive/Board level</li> <li>Monitoring of project activities, plans and outcomes</li> <li>Budget reporting and management</li> </ul>	Principal, VPC&A

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

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility
<b>2</b>	<b>Financial</b>									
<b>2.1</b> <b>F&amp;P</b>	Change in SFC Funding Methodology and Allocation – Reduction in Funding	3	3	9	<ul style="list-style-type: none"> <li>Negotiation/influence at national level</li> <li>Contingency plans for reduced funding</li> </ul>	2	3	6	<ul style="list-style-type: none"> <li>Advance modelling of new funding methodologies and allocations</li> <li>Monitoring impact of changes</li> <li>Amendment of strategic or operational direction/plans</li> <li>Financial strategy sensitivities</li> </ul>	VPCS
<b>2.2</b> <b>F&amp;P</b>	Failure to achieve institutional sustainability	5	4	20	<ul style="list-style-type: none"> <li>Protection of funding through dialogue with SFC</li> <li>Robust annual budget-setting and multi-year financial strategic planning</li> <li>Effective budgetary control</li> <li>Where required, swift action to implement savings</li> </ul>	4	3	12	<ul style="list-style-type: none"> <li>Monthly monitoring of budgets</li> <li>Regular review of financial strategy and non-core income sensitivity</li> <li>Detailed monitoring of savings programmes</li> </ul>	VPCS
<b>2.3</b> <b>F&amp;P</b>	National outcomes on salaries and conditions of service outstrip ability to pay	4	4	16	<ul style="list-style-type: none"> <li>Influence within Employers Association</li> <li>Management of staffing expenditures</li> </ul>	4	3	12	<ul style="list-style-type: none"> <li>Expenditure modelling</li> <li>On-going discussions with staff</li> <li>Financial strategy sensitivities</li> <li>Workforce planning</li> </ul>	VPP&P, VPCS

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



Post Holders	ELT	Executive Leadership Team	Prin	Principal	Score	Impact	Likelihood
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
2	Financial (cont)									
2.4  A&R	Financial Fraud	4	3	12	<ul style="list-style-type: none"><li>Strong financial controls: segregation of duties and review of transactions.</li><li>Review of impact of any changes in structure or duties</li><li>Whistleblowing arrangements</li></ul>	3	2	6	<ul style="list-style-type: none"><li>Continuous review of financial controls</li><li>Internal Audit programme</li></ul>	VPCS
2.5  F&P	D&A Foundation refuses/withholds funding for key College priorities	5	3	15	<ul style="list-style-type: none"><li>On-going dialogue with Foundation Trustees</li><li>Appropriate bid arrangements in place</li></ul>	3	2	6	<ul style="list-style-type: none"><li>Monitor and advise Board of Management</li></ul>	Prin & VPCS
2.6  F&P	Demands of capital developments / maintenance impacts on financial sustainability or delivery of learning and/or services	3	2	6	<ul style="list-style-type: none"><li>Multi-year estates strategy and capital planning</li><li>Lobbying of SFC on capital and backlog maintenance funding</li><li>Planning for D&amp;A Foundation bids</li></ul>	2	2	4	<ul style="list-style-type: none"><li>Monitoring of capital plans and expenditures</li><li>Regular review of capital plans/timescales relative to funds</li></ul>	VPCS

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



<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
<b>3</b>	<b>People and Performance</b>									
<b>3.1</b> <b>LT&amp;Q</b>	Failure to reach aspirational standards in learning, teaching and service delivery	4	3	12	<ul style="list-style-type: none"> <li>Clear quality arrangements and priority actions</li> <li>Continuous self-evaluation and action planning</li> <li>Rigorous CPD arrangements in place</li> <li>Regular classroom observation and learner feedback arrangements</li> </ul>	3	2	6	<ul style="list-style-type: none"> <li>Comprehensive monitoring of key PIs and student/staff feedback</li> <li>Regular Stop and Review events</li> <li>External review and validation findings</li> </ul>	VPC&A, VPP&P, DirC&A
<b>3.2</b> <b>LT&amp;Q</b>	Failure to achieve/maintain compliance arrangements, e.g. contracts; awarding bodies; audit.	4	3	12	<ul style="list-style-type: none"> <li>Robust strategic planning and monitoring</li> <li>Effective environmental scanning</li> <li>Strong partnerships</li> <li>Clear links between strategy and practice</li> <li>Concerted demands for increased activity levels</li> </ul>	2	2	4	<ul style="list-style-type: none"> <li>Effective internal monitoring/review/verification arrangements</li> <li>External review findings</li> </ul>	VPP&P, VPC&A
<b>3.3</b> <b>A&amp;R</b>	Legal actions; serious accident; incident or civil/criminal breach	4	5	20	<ul style="list-style-type: none"> <li>Adherence to legislative and good practice requirements</li> <li>Positive Union relations and staff communication</li> <li>Effective management development programmes</li> </ul>	3	2	6	<ul style="list-style-type: none"> <li>Monitoring and reporting in key areas – eg H&amp;S, equalities, employee engagement</li> <li>Continuous professional development</li> <li>Internal audit programme</li> <li>Staff surveys</li> </ul>	Prin, VPP&P, VPCS, HoE

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

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
<b>3</b>	<b>People and Performance (cont.)</b>									
<b>3.4</b> <b>HR&amp;D</b>	Failure to meet the aspirational standards in respect of the health, safety, wellbeing and development of staff and students	3	4	12	<ul style="list-style-type: none"> <li>Clear and proactive approaches to managing and promoting health, safety and wellbeing</li> <li>Continuous self-evaluation and action planning</li> <li>Rigorous CPD arrangements in place</li> <li>Regular staff and learner feedback arrangements</li> </ul>	3	2	6	<ul style="list-style-type: none"> <li>Regular employee engagement monitoring</li> <li>Open communication with staff</li> <li>Comprehensive monitoring of key PIs and student/staff feedback</li> <li>Regular union/management dialogue</li> </ul>	VPP&P, VPCS
<b>3.5</b> <b>Board</b>	Reputational Risk – Loss of reputation with key stakeholders	4	3	12	<ul style="list-style-type: none"> <li>Marketing strategy</li> <li>Reputation plan</li> <li>Positive marketing approaches</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Stakeholder engagement</li> <li>Social media monitoring arrangements</li> </ul>	VPC&A, DirC&A
<b>3.6</b> <b>HRD</b>	National bargaining outcomes impact adversely on College operations, activity and flexibility	4	4	16	<ul style="list-style-type: none"> <li>Influence within Employers Association</li> <li>Management of bargaining outcomes and implementation</li> </ul>	4	3	12	<ul style="list-style-type: none"> <li>Positive union relations and staff communication</li> <li>On-going discussions with staff</li> <li>Innovation in approaches</li> </ul>	VPP&P, VPC&A

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

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
<b>3</b>	<b>People and Performance (cont.)</b>									
<b>3.7</b> <b>HRD</b>	Industrial Relations Problems (including industrial action)	4	5	20	<ul style="list-style-type: none"> <li>Adherence to legislative and good practice requirements</li> <li>Positive Union relations and staff communication</li> <li>Effective management development programmes</li> <li>Industrial action continuity planning</li> </ul>	4	3	12	<ul style="list-style-type: none"> <li>Regular union/management dialogue</li> <li>Regular employee engagement monitoring</li> <li>Open communication with staff</li> <li>Industrial action continuity planning</li> </ul>	VPP&P
<b>3.8</b> <b>A&amp;R</b>	Breach of data security / data protection	5	4	20	<ul style="list-style-type: none"> <li>Effective management of GDPR compliance</li> <li>Mandatory staff CPD and awareness raising on data protection (relative to role)</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Active data protection monitoring and auditing</li> <li>Effective information and data security policies in operation</li> <li>Regular data security monitoring/testing</li> <li>GDPR Action Plan</li> <li>Staff CPD</li> </ul>	VPC&A, HoICT
<b>3.9</b> <b>HRD</b>	Failure to meet Prevent and related obligations	5	3	15	<ul style="list-style-type: none"> <li>Prevent training</li> <li>Staff awareness and contingency planning</li> <li>Engagement/practice sharing with local agencies</li> </ul>	5	1	5	<ul style="list-style-type: none"> <li>Business Continuity Plan including scenario testing</li> <li>Information sharing with local agencies</li> </ul>	VPC&A, VPP&P

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

Post Holders	ELT	Executive Leadership Team	Prin	Principal	Score	Impact	Likelihood
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
3	People and Performance (cont.)									
3.10 HRD	College arrangements do not minimise risk associated with Modern Slavery	4	3	12	<ul style="list-style-type: none"> <li>Clear and compliant procurement arrangements and procedures</li> <li>Staff identity checking arrangements and use of PVG.</li> </ul>	4	1	4	<ul style="list-style-type: none"> <li>Annual procurement monitoring/reporting</li> <li>Regular employee engagement monitoring</li> <li>Open communication with staff</li> </ul>	VPC&A, VPP&P

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

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very L kely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility
<b>4</b>	<b>Infrastructure</b>									
<b>4.1</b> <b>A&amp;R</b>	Disasters – eg Fire, MIS Failure, Failure of Emergency Procedures	5	4	20	<ul style="list-style-type: none"> <li>Sound systems of administration</li> <li>Clear fire and disaster recovery arrangements</li> <li>Staff CPD</li> </ul>	5	1	5	<ul style="list-style-type: none"> <li>Business Continuity Plan including scenario testing</li> </ul>	Prin & VPCS
<b>4.2</b> <b>F&amp;P</b>	Failure to achieve ambitions of ICT strategy; strategy and development is ineffective	4	3	12	<ul style="list-style-type: none"> <li>Planning, careful phasing of changes to processes and systems</li> <li>Effective management of ICT arrangements</li> <li>Clear investment plan</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Regular review/reporting on milestones, systems effectiveness etc</li> <li>Regular CPD</li> </ul>	VPC&A, HoICT
<b>4.3</b> <b>A&amp;R</b>	Breach of ICT/Cyber security	4	3	12	<ul style="list-style-type: none"> <li>Effective management of ICT arrangements</li> <li>Active ICT/data security monitoring and cyber security policy</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Staff CPD on cyber security issues</li> <li>Regular security monitoring/testing</li> <li>Cyber resilience plan</li> </ul>	VPC&A, HoICT
<b>4.4</b> <b>A&amp;R</b>	ICT infrastructure fails to support effective data security / data protection	5	3	15	<ul style="list-style-type: none"> <li>Effective infrastructure and systems design and implementation</li> <li>Effective management of ICT arrangements and GDPR compliance</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Active data protection monitoring and auditing</li> <li>Effective information and data security policies in operation</li> <li>Regular data security monitoring/testing</li> </ul>	VPC&A, HoICT

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





# STRATEGIC RISK REGISTER COVID 19 SPECIFIC MITIGATIONS

2020 - 2021

As at March 2021

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT			POST MITIGATION EVALUATION			Lead Responsibility
	Risks	Impact	Likelihood	Score	Additional COVID 19 Mitigation Actions	Impact	Likelihood	Score	Additional COVID 19 Monitoring	
<b>1</b>	<b>Strategic and Structural</b>									
<b>1.1 LT&amp;Q</b>	Failure of College strategy to meet the needs of the D&A Region and/or national priorities (eg Employability, DYW, attainment, articulation)	4	4	16	<ul style="list-style-type: none"> <li>Regular strategic analysis and assessment of need for change</li> <li>Strong engagement with government and key partners – influencing national priorities</li> <li>Clear prioritisation of activities</li> <li>Focus on core business</li> </ul>	4	3	12	<ul style="list-style-type: none"> <li>Regular monitoring of recruitment, retention, ROA Outcomes and key strategic needs by SLT and reporting to Chairs</li> <li>Amendment of strategic direction/ plans</li> <li>Rolling curriculum, activity and priority review and implementation of new approaches/services where needed</li> <li>Engagement with government and other partners</li> </ul>	Prin & Chair
<b>1.4 Board</b>	Difficulties or over commitment arising within large scale/national College led initiatives or projects impact negatively on: <ul style="list-style-type: none"> <li>Ability of the College to meet key regional strategies/objectives</li> <li>Financial loss or unmanageable financial risk</li> <li>Reputational loss</li> </ul>	4	3	12	<ul style="list-style-type: none"> <li>Clear prioritisation of activities</li> <li>Effective project/activity management in place</li> <li>Strong engagement with partners/funders</li> <li>Clear governance structures</li> <li>Project/initiative finances clearly understood and reviewed regularly</li> <li>Project cessation, pausing or contingency planning in place</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Regular project updates at Executive/Board level</li> <li>Monitoring of project activities, plans and outcomes</li> <li>Budget reporting and management</li> </ul>	Principal, VPC&A

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

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility
2	Financial									
2.2 F&P	Failure to achieve institutional sustainability	5	4	20	<ul style="list-style-type: none"><li>Protection of funding through dialogue with government, SFC and other funders</li><li>Robust and effective budgetary control</li><li>Where required, swift action to implement savings</li><li>Increased focus on cash position</li></ul>	4	3	12	<ul style="list-style-type: none"><li>Monthly monitoring of budgets</li><li>Engagement with government and other partners</li><li>Detailed monitoring of income optimisation and savings programmes</li></ul>	VPCS
2.4 A&R	Financial Fraud	4	3	12	<ul style="list-style-type: none"><li>Revised financial controls: segregation of duties and review of transactions.</li><li>Review of impact of changes in ways of working, authorisation arrangements</li><li>Whistleblowing arrangements</li></ul>	3	2	6	<ul style="list-style-type: none"><li>Continuous review of financial controls and revised arrangements</li></ul>	VPCS

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



<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
<b>3</b>	<b>People and Performance</b>									
<b>3.1</b> <b>LT&amp;Q</b>	Failure to reach aspirational standards in learning, teaching and service delivery  <b>Post mitigation likelihood still increased beyond normal level due to COVID impact &amp; deferrals</b>	4	3	12	<ul style="list-style-type: none"> <li>Clear input and engagement with revised quality arrangements and priority actions</li> <li>Rigorous CPD arrangements in place to support new ways of working</li> <li>Regular learner feedback and engagement arrangements</li> </ul>	3	4	12	<ul style="list-style-type: none"> <li>Comprehensive monitoring of engagement of learners in learning (where possible)</li> <li>Engagement with revised quality arrangements</li> <li>Outcome monitoring</li> </ul>	VPC&A, VPP&P, DirC&A
<b>3.2</b> <b>LT&amp;Q</b>	Failure to achieve/maintain compliance arrangements, e.g. contracts; awarding bodies; audit.	4	3	12	<ul style="list-style-type: none"> <li>Engagement and communication strategy with compliance bodies</li> <li>Clear input and engagement with revised quality arrangements and priority actions</li> <li>Prioritisation of activities/outcomes</li> </ul>	3	2	6	<ul style="list-style-type: none"> <li>Effective internal monitoring/review/verification arrangements</li> <li>Engagement with revised quality arrangements and contingency plans</li> <li>Outcome monitoring/recording</li> </ul>	VPP&P, VPC&A

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

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS				TREATMENT	POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
3	People and Performance (cont.)									
3.4 HR&D	Failure to meet the aspirational standards in respect of the health, safety, wellbeing and development of staff and students	3	4	12	<ul style="list-style-type: none"><li>• Clear and proactive approaches to supporting and promoting health, safety and wellbeing when WFH and/or on-site</li><li>• Project 2020 developments and mitigations</li><li>• Outbreak management plan</li><li>• Enhanced awareness of challenges/support needs</li><li>• Extensive CPD arrangements in place – Home Working Hub</li><li>• Regular staff and learner feedback arrangements</li></ul>	3	3	9	<ul style="list-style-type: none"><li>• Regular employee engagement monitoring</li><li>• Maintaining and reporting on physical distancing measures</li><li>• Open communication with staff</li><li>• Monitoring of formal and informal feedback – student and staff feedback</li><li>• Regular union/management dialogue</li></ul>	VPP&P, VPCS
3.5 Board	Reputational Risk – Loss of reputation with key stakeholders  Post mitigation likelihood increased outwith College control due to COVID impact on delivery/outcomes	4	3	12	<ul style="list-style-type: none"><li>• Marketing strategy</li><li>• Reputation plan</li><li>• Positive marketing approaches</li><li>• Outbreak management communications plan</li></ul>	4	3	12	<ul style="list-style-type: none"><li>• Positive marketing plan</li><li>• Regular stakeholder engagement</li><li>• Social media engagement and monitoring arrangements</li></ul>	Prin DirC&A

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

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very Likely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Lead Responsibility
<b>3</b>	<b>People and Performance (cont.)</b>									
<b>3.7</b> <b>HRD</b>	Industrial Relations Problems (including industrial action)	4	5	20	<ul style="list-style-type: none"> <li>Adherence to legislative and good practice requirements</li> <li>Positive Union relations and staff communication</li> <li>Effective management engagement and support</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Regular union/management dialogue</li> <li>Open communication with staff</li> <li>Effective management engagement and support</li> </ul>	VPP&P
<b>3.8</b> <b>A&amp;R</b>	Breach of data security / data protection	5	4	20	<ul style="list-style-type: none"> <li>Effective management of GDPR compliance</li> <li>Additional awareness raising of WFH risks</li> <li>Mandatory staff CPD and awareness raising on data protection (relative to role)</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Active data protection awareness raising</li> <li>Effective information and data security policies in operation</li> <li>Regular data security monitoring/testing</li> <li>Staff CPD</li> </ul>	VPC&A, HoICT
<b>3.12</b> <b>HRD</b>	Significant or catastrophic Covid 19 outbreak/infection rate impacts on ability to deliver learning, teaching or other core services	4	3	12	<ul style="list-style-type: none"> <li>Clear scenario and contingency planning</li> <li>COVID 19 H&amp;S mitigations in place, monitored and adapted where required</li> <li>All appropriate government guidance followed</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Monitoring of COVID 19 cases and absences</li> <li>Outbreak management arrangements</li> <li>Amendment to support prioritised services</li> </ul>	Prin VPC&A

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

<b>Post Holders</b>	ELT	Executive Leadership Team	Prin	Principal	<b>Score</b>	<b>Impact</b>	<b>Likelihood</b>
	SLT	Senior Leadership Team	DirC&A	Directors of Curriculum & Attainment	1	Routine	Remote
	Board	Board of Management	HoICT	Head of ICT	2	Minor	Unlikely
	VPP&P	Vice Principal People & Performance	HoE	Head of Estates	3	Significant	Possible
	VPCS	Vice Principal Corporate Services	Chair	Chair of the Board of Management	4	Major	Probable
	VPCA	Vice Principal Curriculum & Attainment			5	Critical	Very L kely

Risk Number & Committee	POTENTIAL CONTRIBUTING FACTORS			TREATMENT		POST MITIGATION EVALUATION				
	Risks	Impact	Likelihood	Score	Mitigation Actions	Impact	Likelihood	Score	Monitoring	Responsibility
<b>4</b>	<b>Infrastructure</b>									
<b>4.3</b> <b>A&amp;R</b>	Breach of ICT/Cyber security	4	3	12	<ul style="list-style-type: none"> <li>Effective management of ICT arrangements</li> <li>Active ICT/data security monitoring and cyber security policy</li> <li>Additional awareness raising of WFH risks and COVID related 'scams'</li> </ul>	4	2	8	<ul style="list-style-type: none"> <li>Staff awareness raising/CPD on cyber security issues</li> <li>Regular security monitoring/testing</li> <li>Cyber resilience plan</li> </ul>	VPC&A, HoICT
<b>4.6</b> <b>LT&amp;Q</b>	ICT/Cyber failure significantly disrupt learning, teaching or other core services	4	3	12	<ul style="list-style-type: none"> <li>'Cloud first' strategy implementation for major services/systems</li> <li>Clear and robust management of ICT systems</li> </ul>	3	1	3	<ul style="list-style-type: none"> <li>Systems monitoring</li> <li>On-going cyber resilience and systems development</li> </ul>	HoICT

**BOARD OF MANAGEMENT**

**Audit & Risk Committee**

**Tuesday 9 March 2020**

---



**Information & Cyber Security Risk**

**PAPER I**

**Sensitive and Confidential**

**Not to be Published**