



HUDDERSFIELD NEW COLLEGE FURTHER EDUCATION CORPORATION

Audit Committee held on Tuesday 21st March 2017 from 5pm.

Confirmed Minutes

- Present:** Mr A Nelson (Chair), Ms H Haigh, Mr K Webb and Mr N Uppal (100%)
- In attendance:** Mr A Shaw, Mr D Scott (Wylie & Bisset), Mr A McCulloch (Tiaa), Ms J Pryce and Ms R Sutcliffe.
- Clerk:** Mrs C Coupland

1. Apologies for Absence/ Declaration of Interest

No apologies had been received.

There were no declarations of interest.

2. Minutes from Meeting held on 28th November 2016

Resolved:

- That these be accepted as a correct record.

3. Matters arising

There were no matters arising.

4. BAF Assurance Review: Breaches to IT Security, Unlawful access to data, loss of network connectivity or service.

Ms Pryce and Ms Sutcliffe explained that the outcome of the ICT High Level Health Check (to be discussed in agenda item 5) prompted a review of the risk title and overall risk scores. It has since been reframed to extend to breaches of IT Security and unlawful access to data. The increase in risk scores reflected the broadened scope of this particular risk and the additional risks inherently associated with any threat of cyber-attacks. The committee agreed with the rationale presented but were mindful that the 'loss of college data' element of the original risk had been omitted. Ms Pryce explained that this was an oversight and agreed it necessary to reinstate this specific element into the scope of the current risk.

Members used this opportunity to further scrutinise the assurance report submitted jointly by Ms Sutcliffe and Ms Pryce. The Committee was particularly interested in how the college is preparing for the General Data Protection Regulation (GDPR). Ms Pryce confirmed that management are aware that the law is changing with the GDPR expected to be coming into force in mid-2018. Ms Pryce confirmed that she and Ms Sutcliffe are to be mapping out which parts of the GDPR will have the greatest impact on the college and will give those areas due prominence in the overall planning process and risk management review. Further analysis of the GDPR and specific impact on this risk shall be reflected, where necessary, in the updated Board Assurance Framework which is to be presented at the next Committee meeting.

After a robust discussion members were confident in the mitigating actions being taken by the college. Furthermore, the committee was satisfied with the different assurances identified within the Board Assurance Framework for the risk. The Committee therefore agreed that an overall green assurance level shall continue to be assigned to this particular risk.

Ms Pryce also presented the IT Disaster Recovery Plan and the IT Business Continuity Plan for review by the Committee. The Disaster Recovery Plan details the college policies and procedures for an IT related disaster recovery as well as HNCs process-level plans for recovering critical technology platform and the telecommunications infrastructures. The IT Business Continuity Plan details the procedures in relation to IT business continuity and summarises HNC's recommended continuity. Both Plans have recently been reviewed and approved by the Senior Leadership Team. The Committee agreed that the plans presented were comprehensive – Members were also satisfied that the identified Recovery Time Objectives (*RTO - duration of time which a business process must be restored after disruption to avoid unacceptable consequences associate with a break in business continuity*) and Recover Point Objectives (*RPO- Maximum tolerable period in which data might be lost from an IT service due to an incident*) would enable the college to quickly create a restore schedule, with services retrieved, that would be responsive to business need and to business cycle .

With reference to one of the recommendations cited within the ICT audit report - Ms Pryce welcomed committee members' views on whether arrangements should be made to hold copies of back-up data offsite – by use of Cloud storage or a specialist Disaster Recovery contractor or data centre. Following the audit, the Senior Leadership Team are reviewing options for this area - however to date management have been satisfied that critical data is protected as the colleges Disaster Recovery (DR) Server room is located in another campus building to that of the Live and Central server rooms. To date the college's position has been that the likelihood of a major disaster incident, affecting both buildings, did not justify the costs implications of creating a full DR suite off site. Members were in agreement with management given the presented cost projections to secure against major incidents; however all agreed it useful to scope the options and costs associated with creating an off-site data back up only system. It was agreed that this approach may be beneficial given the possibility that access to the whole of the college campus could be restricted for a period of time following an incident to any one building; albeit that remote access options would always be available.

Members also wondered whether possible disaster recovery options - in particular off-site data back up only systems - could be available through the Collaborative Learning Trust, with cost sharing opportunities being identified for all colleges and/or the University.

The Committee was advised that the IT Disaster Recovery Plan and IT Business Continuity Plan shall continue to be subject to bi-annual reviews.

Resolved:

- **To assign Green Overall assurance to the risk**
- **For the Clerk to update the Master BAF.**
- **To receive the IT Business Continuity Plan and IT Disaster Recovery Plan**
- **For the College to explore the costs associated with off-site data back up only systems and the viability of storing such data with reciprocal education providers.**

Ms Sutcliffe left the meeting at this point.

5. Internal Audit Reports

Mr McCulloch presented his reports to the Committee.

Information Communications Technology (ICT) High Level Health Check

This review considered the high level arrangements operating in relation to ICT Disaster Recovery Plan, ICT management Controls and ICT Network Security. The overall assurance assessment assigned was reasonable assurance.

As a result of the audit – 4 important and 4 routine action points were recommended. All actions have been accepted by management - implementation dates and responsible officers have been identified and listed within the final report. Members were in agreement with the management's responses.

It was noted that the audit findings report did not provide any relevant benchmarking data for comparative purposes. Mr McCulloch explained that at the time of the report no other comprehensive ICT reviews had been undertaken. However he was now in a position to confirm that a recent (and similar) review had since concluded with 13 urgent and 2 important recommendations being made. In light of this information the committee agreed that this audit provided substantial assurance to the corporation. It was also noted that the college had been audited against ISO27002 - which is the international standard for Information Security Policies which provides a comprehensive set of controls for sound practice in information security.

Assurance Review of the Teaching, Learning Assessment Arrangements.

This review considered the Teaching Learning Assessment (TLA) Strategy and related Continuous Professional development (CPD) and the new appraisal framework and associated arrangements introduced by the College in 2016. The review also considered the pilot run for 2015/16 and tested for compliance with the requirements of the framework. The overall assurance assessment assigned was reasonable assurance.

Key findings of the report were:

- The college has a detailed framework for the TLA arrangements
- The processes and requirements for the appraisal elements for both the appraisee and appraiser are clear and have been communicated to all staff.
- Testing did however identify some missing data for the current round of appraisals which need to be recorded within College IP (the college's electronic recording and management system) to ensure that the base information is correct.

2 important action points were recommended and have since been accepted by the college for implementation.

Resolved:

- **To receive the reports**
- **To congratulate all staff on the positive audit findings**

Ms Pryce left the meeting at this point.

6. Recommendation tracking

Mr Nelson asked the Committee to note that this was a standing agenda item.

Mr Shaw subsequently confirmed that there have been no further Internal Audits undertaken since the Committee last met. As reported at the last meeting, all recommendations on the tracker have been completed but will remain on the tracker until the follow-up audit confirms this to be the case. The follow up audit will not be undertaken until May/June 2017. The tracker will however now be updated with the accepted recommendations from the two recent audits.

Resolved:

- **To receive the report**

7. The Post 16 Audit Code of Practice

The Clerk informed members of the Committee that the post-16 audit code of practice sets out the Education Funding Agency (EFA) revised assurance and accountability requirements for post-16 providers for all periods commencing on or after 1 August 2016.

The Post 16 Audit Code of Practice includes updated guidance on the annual assurance arrangements for sixth-form and further education colleges and their auditors. The Clerk drew members' attention to the changes in this version.

To support corporations in drafting the statement of regularity, propriety and compliance, the EFA will once again publish a self-assessment questionnaire. The self assessment questionnaire will however be published in due course following further consultation with the sector and will again be a required element of the Regularity Audit.

The Clerk confirmed that the Audit Committee's current terms of reference continue to reflect the accepted good practice for audit committees of publicly funded organisations as set out within the Post 16 Audit Code of Practice 2016-2017.

Resolved:

- **To receive the report**

8. External Audit Strategy and Planning Memorandum

Mr Douglas presented his report to the Committee.

The purpose of the report explained the scope of the Audits of the financial statements and regularity, the proposed audit approaches and highlighted the key risks that Wylie & Bissett will be focussing the external audit work upon.

The Committee considered and agreed to the timetable and communication plan proposed to ensure timely audit findings report.

Resolved:

- **To approve the External Audit Strategy and Planning Memorandum**
- **For the Clerk to confirm dates of meeting for the Autumn Term of 2017/18, once agreed.**

9. Confidential Reporting Code and Policy

The Committee agreed with the Clerk's assessment that the current policy reflects good practice initiatives and is currently procedurally compliant with relevant legislation for how the college is to manage and respond to any raised concerns.

The Clerk however proposed the following additions to the existing policy to reflect recent amendments to "Keeping Children Safe in Education" (Sept 2016) and the revised Government Guide on Whistleblowing for employees (March 2017):

- i) For section 2 Scope of Policy to cite the additional concerns to be covered within the whistleblowing policy as specifically mentioned within the two documents referenced above.
- ii) For section 7.1. to make reference to the additional contact points now available as raised within the two documents.

The Committee reminded itself that Whistleblowing policies and procedures need to be clearly communicated to employees and students for the College to be in a position to prove that it has taken all reasonable steps to prevent whistle-blowers from being subjected to an unlawful detriment. The Clerk confirmed that the revised policy (once approved by the Corporation) shall be made available to all via the website and via Moodle (the college's virtual learning environment). The Clerk shall also email all students and staff members directly advising them as to the purpose of this policy and where to access it.

Resolved:

- **That the changes to the policy be recommended for approval by the Corporation.**

10. Any other Business.

Board Assurance Review (BAF); Mid-Year Review.

The Clerk informed the Committee that the Senior Leadership Team have identified that the key strategic risks within the college's risk register needs to be reviewed and updated in light of the new strategic plan and objectives going forward.

The Clerk informed the committee that the planned review of the BAF, in its entirety, shall now take place at the Committee's next meeting scheduled for June 2017. The annual review of the College's Risk Management Policies and Procedures shall also be submitted at this meeting.

11. Learner Impact Reflection

The impact of discussions and scrutiny of the Committee work in improving the outcomes and experience for all learners was considered and the following agreed:

- **This Confidential Reporting Code provides a procedure whereby possible malpractice can be disclosed in confidence and without prejudice or retribution by any staff member, student or governor thus ensuring that HNC continues to be a positive place to work and study.**
- **The IT Disaster Recovery Plan and IT Business Continuity Plan assures the Committee that the College is able ensure the security of students' personal data and that HNC has sector leading and stable IT networks to support students learning**
- **By ensuring infrastructure plans for resilience are in place HNC can continue to provide the best learning experience and environment for all students and staff as well as protect critical business functions in case of a disaster.**
- **The overall audit opinion provides assurance that the college has an adequate and effective framework for governance, risk management and internal control.**
- **Ensuring that the College is maintaining the quality of learning to maximise the Student Learning, Experience and Outcome.**
- **Assurance received that the college remains compliant with regularity and propriety requirements as per the terms and conditions of funding.**

12. Determination of confidentiality

The appendices for the IT Disaster Recovery Plan and IT Business Continuity Plan were deemed to be confidential given the sensitive nature of information detailed.

13. Date of next meeting: Tuesday 13th June 2017 at 5pm.