CARDINAL NEWMAN COLLEGE

BOARD OF GOVERNORS – AUDIT COMMITTEE

A meeting of the above Committee was held at **4.00 p.m.** on **Wednesday 3 March 2021** on Microsoft Teams.

Members present:
Peter Halpin (F), Chair
Peter Towers (F), Vice Chair
Charu Ainscough
Bernadette Davies (F)
Bob Eastwood (F)

Officers in attendance
Nick Burnham, Principal
Bob Deed, Clerk
Katie O'Reilly, Vice Principal Finance & Resources
Claire Riding, College Accountant

MINUTES

1. Opening prayer

The meeting commenced with a prayer.

2. Welcome, introductions and apologies

There were no apologies to be recorded.

3. Declarations of interest

There were no declarations of interest.

4. Minutes of the meeting on Wednesday 11 November 2020

The minutes of the meeting of the Committee held on Wednesday 11 November 2020 were confirmed as a true record.

5. Matters arising from the minutes

There were no matters arising not covered elsewhere on the agenda.

6. Update on cyber-risks (taken after item 4)

Steve Gray and Anthony Dickinson of the Network Team presented on

- Issues raised by the National Cyber Security Centre (NCSC) presentation on cyber risks which they attended through invitations obtained by Bob Eastwood.

- Developments at the College on cyber security.

The NCSC presentation and guidance highlighted the risks of compromised email and the importance of Multi Factored Authentication (MFA). The College has implemented strong controls but Network staff are mindful of the needs of staff and students. For example, MFA is required from computers outside the College but not on the College site. Similarly access to the system is not allowed from abroad unless there are visits to particular countries.

The NCSC recommend anti-spoofing technical controls which the College has in place. The College is aware of the risks of Hyper-Targeted Attacks (e.g. spear fishing, impersonation) and Opportunistic Attacks (e.g. phishing, ransomware). Barracuda Sentinel has stopped 593 attacks since the College installed it. As discussed before, the College uses Microsoft Advanced Threat Protection which checks on attachments and links before they can be accessed by a College email account.

Ransomware is a growing threat including for the education sector. The College has extensive arrangements, including Intune device management and Window Defender anti-virus, to address the threat.

Disaster Recovery is another key theme flagged by the NCSC. The College has a strategy of moving cloud services which have good security and opportunity for recovering data if attacked. Cloud back-up is supplemented by secondary cloud-to-cloud arrangements.

The NCSC recommend good practice on passwords. The College has aligned its requirements in line with this.

The College is moving forward on cyber security on a number of fronts:

- Cedar - commissioning a review of Cedar application-level security this month; an action plan will be produced with a Cedar developer dedicated to work through any changes required – urgent changes completed as a priority; other changes before 31 July.

- Implementation of a software repository to allow staff to install software on their College devices from a managed software store.

- Reviewing administrator privileges de-escalation/escalation on requirement.

- Reviewing firewall/perimeter equipment/services.

- Progressing through Cyber Essentials and looking towards Cyber Essentials Plus.

The Chair asked about the implications of home working. The Network Manager explained that the existing controls stretched over devices off-site. He said that the firewall/perimeter review would consider this.

The Chair asked about whether the Cedar security review would address the development of the software. The IT and Development Manager said that this would be part of the scope.

A governor asked about the risks of infection from governors' equipment. The IT and Development Manager said that the cloud software protected the College in this scenario. Likewise, when students had infected equipment.

A governor asked about the risks from students. The IT and Development Manager acknowledged that this was a threat and said that there had been cases in the past. He said that reliance could be placed on the College's investment in defences from leading IT businesses such as Microsoft.

A governor asked about the timing of the Cyber Essentials accreditation. The Network Manager said that the Cyber Essentials was essentially paper-based with the self-assessment being completed. After accreditation, the College could then progress to Cyber Essentials Plus. He said that the College already commissioned penetration testing.

A governor said about her bad experience of Zoom meeting being hijacked. The IT and Development Manager said that at the start of the pandemic the College had been aware of the risks associated with Zoom after they had been highlighted to colleges and universities by the consultancy JISC.

7. Presentation on funding risks

The Clerk as Vice Principal Finance & Resources outlined the context of funding audit risks. He said that in the 1990s and early 2000s, all colleges had audits of student numbers and then Individualised Student Records. From 2004/5 these audits were replaced by lighter-touch regularity audits of the regularity and probity of the use of public funds with only a sample of colleges (principally higher-risk FE colleges) having funding audits with the risk of funding being clawed back. He said that very few sixth form colleges have had a funding audit although that could change.

The Vice Principal Finance & Resources highlighted the main themes covered by funding audits:

- the existence and eligibility of students recorded on the individualised learner record;
- the supporting documentation for data;
- the compliance with funding requirements.

The slides set out the risks tested by funding audit. This noted that these were generally very low risk for the College as its provision was classroom-based for full-time students. He noted that residency was occasionally an issue and likely to be more so in the future where EU citizens had not obtained settled status.

The Chair agreed that the risks appeared to be low.

8. Progress report on audit recommendations

The Clerk as Vice Principal Finance & Resources noted that while several recommendations from the Risk Register assurance review had been completed, others were being implemented for governors' meetings in March.

The Committee repeated their concern that when the risk register was considered attention should be focused on strategic and key operational risks with a clearer sense of how risks impacted strategic objectives.

The Committee noted the completion of the remaining GDPR audit recommendation.

9. Update on the assurance plan

The Clerk as Vice Principal Finance & Resources updated the committee on the Network Security assurance review. He said that there had been difficulties arranging a date with the consultancy BTRP. As the College was required by its Funding Agreement with the ESFA to seek Cyber Essentials accreditation, it was agreed with the Chair that this should be undertaken rather than the assurance review. It was noted that the Cyber Essential self-assessment was being validated by the specialist consultancy JISC.

The Chair emphasised that the assurance plan should be a live document and that it should revisited during the year. The Clerk said that the risk register extract highlighting reliance on controls could be brought to the next meeting.

The Committee agreed that the Clerk should bring to the extract of the risk register showing the reliance on existing controls to inform the discussion of priorities for assurance reviews.

10. Risk register – termly update

A governor suggested that the risk register should not include a risk around road traffic accidents as this did not appear to have implications for the College's strategic objectives. Another governor noted the busy roads around the College . He believed that this was a risk for the College to manage and detail on the register.

The Vice Principal Finance & Resources said that the College had in the past had a student fatality. She noted that the College was focused on working with partners to improve safety around the College – both students arriving at and leaving College as well as moving between buildings.

A governor said that the issue might highlight the need for more on the "so what" of how risks related to the strategic objectives. Clerk as Vice Principal Finance & Resources said that he had discussed this with the Chair earlier in the day. He would bring to the next Committee meeting a mapping of risks against the strategic objectives.
The Chair said that there was a risk of overload and missing key risks – "wood for trees" – when 54 risks were listed.

There was discussion about examinations and the risk register. In the light of Teacher Assessed Grades (TAGs) a governor queried why the risk relating to preparedness for new specifications referred to mock exams emulating as far as possible a 'live' experience. It was noted that examinations, including materials from the exam boards, were likely to be used in the TAGs process in the summer.

A governor said that mental health during the pandemic was a real issue for the College. She suggested that the risk should be reviewed. The Link Governor noted the issues and responses of the College.

The Clerk noted that the College had a safeguarding assurance plan on a triennial basis. It would be due in the near future and could include mental health in its scope.

11. Determination of any items to be treated as Confidential

There were no items which required to be treated as confidential in the minutes.

12. Date and time of the next meeting

The next ordinary meeting of the Committee is scheduled to be held at 4.00 p.m. on Wednesday 26 May 2021.