PUBLIC MINUTES OF THE
AUDIT COMMITTEE
25 SEPTEMBER 2025

Present:
Ms A D Berry (External Board Member)
Mr T Burrell (External Board Member)
Mr A Dover (External Board Member, Chair of Audit Committee)
Mr M Fabian (External Board Member)
Ms S McKinlay (External Board Member)
Ms G Read (External Board Member) via Teams

In Attendance:
Mr K Agnew, IT Systems and Security Manager, up to and including item 24/25
Mr D Alma, Health and Safety Manager, up to and including item 23/25
Mr A Bates, Chief Financial Officer
Mr J Billingham, Director of IT and Estates, up to and including item 24/25
Mr M Burgess, Principal
Ms S Dalby, Head of Business Intelligence
Mr J Singleton, IT Operations Manager
Ms H Snelling, Director of People, Facilities and Infrastructure
Ms J Cosson, Head of Governance
Ms L Tweedie, RSM

Apologies:
Mr S Lawrence, Hazlewoods
Mr A Phipps, Hazlewoods

Attendance: 100%

38/25 Opportunity for Private Business (including with Auditors)

Members were given the opportunity to meet with the Auditors in the absence of the Executive. Members and Auditors confirmed that there were no matters of concern that they wished to raise in the absence of the Executive.

39/25 Apologies

Apologies were noted and received as above.

40/25 Declarations of Interest

Members noted those standing declarations currently recorded on the Register of Interests. No new declarations of interest were noted.

41/25 Confidentiality of Items

As marked, due to their commercially sensitive nature, for a period of two years.

42/25 Minutes of the meeting of 11 June 2025

The minutes of the meeting were approved and signed as a true record by the Chair.

43/25 Matters Arising from the Minutes and Actions Matrix

Members reviewed the actions matrix and noted the status update of each item.

44/25 Health and Safety Update and Annual Report

DA presented a comprehensive update on health and safety, highlighting the College's achievement of the ROSPA Gold Award, ongoing accident trends, completed external audits, and actions taken regarding Legionella and training improvements.

DA reported that the College has received the ROSPA Gold Award for health and safety, a significant accomplishment as only three other UK colleges and universities have achieved this on their first attempt. There were some questions about the involvement of governors. The award reflects a collective effort involving governors, the Executive Team, and curriculum teams.

DA informed Members that accident rates, including minor cuts and student illnesses, are consistent with the previous year, with over 50% of first aid cases related to medical issues rather than injuries from College activities.

In terms of external audits and compliance, all legal checks and actions from external audits have been completed. New audits are scheduled for January and February next year, with areas of focus to be included in the next report.

ACTION: AD to be invited to join audits in the new year.

An improvement in training, especially for minibus drivers, was noted. The College has replaced an end-of-life minibus at Cinderford and addressed training gaps by splitting training requirements based on driver needs, expediting the qualification process. Members discussed the merits of face-to-face training and the improvement of online packages.

An ongoing issue with daisy-chaining of extension cables was noticed. DA advised that there is a plan to prevent this.

A Member asked for an update on the management of the ongoing Legionella issue at Cinderford and was informed that there are lower positive readings and a plan to replace flexible pipework under sinks. Additional measures include adjusting hot water temperatures and installing drain valves on expansion tanks, with further sampling scheduled. Members were reminded that the readings are still below reportable levels.

Members reviewed the Health and Safety Annual Report. This will be presented to the October Board meeting along with the Health and Safety Policy.

RESOLVED: The Committee congratulated DA and the College on the ROSPA Gold Award. They commended the progress made in health and safety as described in the Annual Report and noted the current assessment of the College's Health and Safety arrangements.

45/25   Review of Emergency Incident Policy and Procedures

JB outlined the upcoming strategic review of the College's business continuity and crisis management plans, using the College's insurance company, with subsequent scenario-based testing and internal document reviews planned.

JB confirmed that the company will conduct a strategic review of the College's business continuity and recovery plans in early October, providing a report to inform further actions.

Following the strategic review, the same company will be engaged to run a desktop, scenario-based test day, similar to previous cyber exercises, to assess team preparedness and knowledge.

The College is proactively reviewing all relevant paperwork and plans ahead of the external strategic review to ensure readiness and identify any immediate gaps.

A Member inquired whether the College has implemented any additional security measures following recent lockdown incidents at other educational institutions including another college. JB explained that the lessons learned are being reviewed, particularly regarding communication effectiveness and access control, with some additional lockdown measures implemented, but no major changes are deemed necessary at this time based on current assessments.

RESOLVED: The Committee noted the update on the College's Emergency Incident Policy and Procedures.

DA left the meeting.

46/25   AI Update

Following previous discussions at Board, MB introduced a paper prepared by SD setting out the College's approach to AI, including the formation of an AI and Systems Governance Group, risk management, tool approval processes, staff training, and the monitoring of AI use in both teaching and professional services.

SD reported that an AI and Systems Governance Group has been established, including representatives from IT, finance, data protection, safeguarding, and teaching and learning, to oversee internal AI policy development, risk management, and tool approval.

The group maintains a risk log, with cyber and safeguarding identified as the highest risks. A formal process for approving new AI tools has been implemented, requiring

assessment of strategic fit, training needs, resource implications, and data protection considerations before Executive Team approval.

Efforts are underway to develop mandatory, accessible, tailored AI training materials for staff, drawing on external guidance where available e.g. from the DfE, DSIT and JISC. The group is also monitoring external developments and integrating relevant support materials into internal training.

Professional services usage has been reviewed through departmental meetings, identifying needs and barriers. In teaching, AI use is being observed during learning walks and departmental reviews, with a focus on its impact on teaching and learning.

The group evaluates whether approved AI tools use data for training and ensures staff are educated on privacy settings.

A Member asked what AI tools are under consideration. SD replied that several popular AI tools are being trialled along with an internally developed tool and a chatbot on the College website. The College is mainly focusing on tools which offer the most benefit for learners. These are monitored by an academic working group. There is a separate professional services working group looking at the use of LLMs.

Another Member asked if the College has an inventory of existing software used to track AI updates. KA replied that it has, particularly in relation to the finance system. The College is aware of Shadow IT/AI widgets and is monitoring.

Members asked about the process for gathering information on AI usage, wondering how the College is exploring/monitoring what AI staff are using. SD explained that, for professional service teams, a review was carried out last academic year to assess usage with the aim of identifying key requirements and stumbling blocks. In terms of teaching and learning, the Deputy Head of Teaching and Learning participates in departmental meetings and learning walks to observe AI's impact and invites staff to share what tools they are using. MB added that the approach is to encourage staff to use AI effectively to improve teaching and learning. SD reported that the College is preparing an AI insights update for staff, which will be included as part of the Engage staff magazine. This update is intended to provide a FAQ and raise awareness about AI-related topics for staff.

A Member had a question on the risk register, page 64, noting that it rates risk before and after mitigations, but it doesn't actually state what the mitigations are.

ACTION: SD to include the risk mitigations for the next meeting.

Another Member wondered if there was any risk around staff recruitment in terms of applicants using AI to enhance their job applications e.g., CVs.

HS answered that the risk is currently low in the College's context. Surprisingly few applicants appear to be using AI on their application forms at present. The recruitment process is robust and designed to filter out unsuitable candidates with interviews and other checks likely to mitigate any advantage gained from AI-

enhanced applications. The application form is just the first step; further stages in recruitment are likely to reveal genuine suitability. The Committee agreed that, while the risk is not significant now, it is something to keep under review as AI adoption grows.

The Committee discussed concerns about changes to terms and conditions on platforms like Facebook, where users may be prompted to accept new terms via a tick box. It was highlighted that, by ticking such boxes, users might inadvertently give platforms permission to use their data, including potentially confidential information, for AI training purposes. The risk is particularly relevant if staff or students use external platforms for college-related work or upload sensitive documents.

SD responded that the College's approach is to carefully review and approve any external tools for use, specifically checking whether they use uploaded data for training. Staff are being educated about privacy settings and the importance of understanding what permissions they grant when using external platforms. The Committee acknowledged that, while the College can control approved tools and educate staff, it cannot fully influence what learners do on their private accounts. The importance of updating acceptable use policies and ongoing staff/student education was emphasised to mitigate risks.

SD will attend Audit Committee meetings going forward to provide updates on AI governance. TB offered to meet with SD in relation to AI governance as Digital Technology Link Governor.

RESOLVED: The Committee noted the AI Update and the current arrangements for AI governance.

SD left the meeting.

47/25 Cyber Security Update (C)

KA presented the Cyber Security Update.

KA introduced the newly appointed IT Operations Manager, and provided updates on staffing, training, recent penetration testing, password security, Wi-Fi upgrades, and ongoing cyber incident management.

JS outlined his background and specific areas of expertise. Members asked him for his initial impressions of the IT infrastructure at the College. JS reported that there are stricter requirements in education than in many other organisations and that all necessary processes and procedures appear to be in place.

In terms of staffing and team structure, KA reported that the IT team is now fully staffed, with recent hires filling all vacancies despite some staff on leave. JS will also deputise for the Head of IT.

Key IT Team members have completed cyber incident response training with JISC, and KA has presented a college-wide cyber awareness roadshow to keep staff

informed about security practices and the importance of their role in maintaining security, which was well-received.

An external penetration test has been carried out.

The annual CIRP exercise has been completed. TB will be happy to assist with future scenario planning as Digital Technology Link Governor.

KA reported that no significant cyber incidents had been experienced, though daily threats are managed. He advised that the education sector remains disproportionately targeted for cyber-attacks, with ongoing monitoring of student network activity and collaboration with safeguarding teams to address potential risks.

Members asked about sector trends in cybersecurity and, in particular, whether there are any themes coming from the National Cybersecurity Centre at the moment in terms of education, bearing in mind that the education sector typically sees a higher number of reported incidents than others, with an average of four to five colleges affected each year, as shown in NCSC charts and reports. KA advised that the NCSC, along with partners like JISC, regularly warns of increased targeted attacks against UK colleges and universities.

Members noted the importance of monitoring these trends and learning from NCSC guidance and reports. The College's approach is to follow best practice frameworks, such as Cyber Essentials Plus and DfE digital standards, which are aligned with NCSC recommendations. The IT team regularly reviews external assurance and benchmarking against sector best practices, including those set by the NCSC.

A Member asked what external guidance the College follows in terms of the security measures that should be in place. KA replied that the College follows established external frameworks and standards. Specifically, the College adheres to:

- **Cyber Essentials Plus**: This is a government-backed scheme, aligned with National Cybersecurity Centre (NCSC) best practice. Achieving this certification requires meeting a framework of security controls and undergoing external audits.
- **Department for Education (DfE) Digital Standards**: The College ensures its practices meet these standards, which are regularly updated and reflect sector best practice.
- **NCSC Guidance**: The College works closely with sector partners and follows advice and benchmarking from the NCSC, which is the UK's authority on cyber security for education and other sectors.

The College also undertakes regular external audits and benchmarking to ensure its security measures are robust and up to date.

External assurance is included in reports to governors and the Audit Committee, demonstrating that the College's security practices are measured against recognised best practice and not just internal standards.

Members reviewed governor completion of Boxphish training.

RESOLVED: Members noted the Cyber Security Update.

HS, KA, JS and JB left the meeting.

48/25 Internal Audit Reports:

LT presented the internal audit reports, focusing on compliance with Prevent and Protect duties, highlighted areas for improvement in Prevent risk assessments and policy alignment, and delivered an annual opinion confirming adequate governance and control, with benchmarking against sector standards.

Final Report

- **Prevent Duty and Protect Duty**

The audit reviewed compliance with updated Prevent duty guidance and planning for Protect duty (Martyn's Law), identifying three medium-priority actions, notably the need for improved safeguarding and Prevent risk assessments for events and centralised record-keeping.

Recommendations included updating policies and procedures in line with review cycles and aligning the Prevent risk assessment format with the DfE template to demonstrate best practice adherence.

LT understands that these recommendations have already been followed up.

Internal Audit Annual Report 2024/25

The internal audit annual opinion concluded that the College has adequate and effective governance, risk, and control systems. The benchmarking report showed that the College's position is very much in line with sector norms, and the assurance level was considered positive.

RESOLVED: Members noted the internal audit reports

49/25 Risk Management Update, Annual Report and Review of Board Assurance Framework (C)

AB presented the Risk Management Update and BAF.

Members noted increased risks related to UK economic health, political uncertainty, and adult funding, with ongoing strategies to mitigate financial and operational risks.

The risk register had been updated to reflect the increased risk from UK economic health and political uncertainty, particularly regarding potential budget cuts and the impact of future government reforms. Members debated the likelihood and impact of the next government being formed from outside of the traditional parties. MB stated

that these matters will be discussed further at the October Board meeting and at subsequent strategy days.

AB informed Members that strategies to address reductions in adult funding include bidding for new contracts, reducing costs, and launching in-house learner recruitment initiatives. The impact of funding cuts on services for ethnic minorities and refugees was discussed.

In terms of staffing and recruitment challenges, Members asked if the success in filling IT vacancies was reflected across other recruitment. They were informed that, while IT staffing gaps have been filled, other areas such as Construction and Learning Support Assistants face ongoing recruitment challenges due to funding constraints and increased learner number recruitment.

A Member asked for an update on devolution in the context of adult education funding and local government changes. There was mention of recent calls for the 16–19 budget to be devolved. MB advised that the College is monitoring developments around the devolution of the 16–19 education budget and adult funding, which could significantly impact future strategy and operations. The local authority will need to agree on a single proposal for devolution by November (with implementation expected by 2028–29). Discussions are ongoing. The process is complex, with the government requiring only one proposal per local authority, making consensus challenging. The College is considering the implications of devolution for its funding, strategy, and ability to serve learners, especially in the context of possible government reforms and budget cuts. The uncertainty around devolution and its impact on adult funding is a significant operational risk.

It was noted that the Board Assurance Framework had been updated, with all sources of assurance rated as green. Governors were encouraged to review the framework to understand where assurance is derived. The Board Assurance Framework will be submitted to the Board for approval. Members considered that the document summarised the key areas of risk and assurances well.

RESOLVED: Members noted the Risk Management Update and Risk Register.

50/25 **Review of Audit Recommendations Register**

Members reviewed the Audit Recommendations Register (ARR) and received an update from AB as to the status of each item. It was noted that management responses are followed up by the internal auditors.

RESOLVED: Members noted the status of and were satisfied with the Audit Recommendations Register.

51/25 **Management Update on Reportable Events**

There have been no such events since the last meeting.

RESOLVED: The Update on Reportable Events was noted.

52/25 Approval of Policies
- **Health and Safety Policy**

The Health and Safety Policy was reviewed. There had been no significant changes. It will be recommended to the Board in October.

JC reported that the College is updating its anti-fraud policy and procedures to ensure compliance with the Economic Crime and Corporate Transparency Act. The policy is usually reviewed as part of the accountability review at the November Audit Committee meeting but, in view of the focus on fraud by the DfE and the OfS and the importance of the Act, the policy will be submitted it to the full Board at the October Board meeting and referenced at the November Audit meeting.

LT informed Members that the Act includes strict liability for benefiting from fraud.

Members discussed the implications of the Act, noting the need for robust anti-fraud procedures, staff training, and policy updates to ensure compliance and mitigate organisational liability. AB reported that new staff are required to sign a code of conduct and receive training on fraud prevention, with particular emphasis on key roles and adherence to tendering and procurement procedures.

RESOLVED: The Health and Safety Policy was approved for recommendation to the Board. The update on the Anti-Fraud and Corruption Policy was noted.

53/25 Key Items for GC Board

The Key Items for Board were discussed, noting any risks to be added/highlighted on the Risk Register.

- ROSPA Gold Award.
- Full IT team.
- Annual Internal Assurance Opinion – Reasonable Assurance.
- First AI Update to the Committee.

Recommendations from Audit Committee to the Board/other committees

- Health and Safety Policy.
- BAF.

Risks to be highlighted/added to the College's Risk Register

- As per the Risk Register.

54/25 Any Other Business

None.

55/25 Date and Time of Next Meeting

25 November 2025, 5pm, Gloucester campus, C126e.

Signed   *MA Fabian*

Date   25.11.25