NORTHERN REGIONAL COLLEGE

RESOURCES COMMITTEE

Meeting on 26 March 2026 on Microsoft Teams at 3.45pm.

Present: Mr I Murphy (Chair), Mr M Higgins, Ms D McIlwaine, Mr B Patterson

In Attendance: Mrs C Brown, Dr P Graham, Mr S Laverty, Mr J Ross, Mrs K Wallace (Secretary)

External Presenter: Mr B McCluggage

47.1 Apologies

No apologies.

47.2 Declaration of Interests

None.

47.3 Cyber

The Committee received a detailed presentation from BMC providing an assessment of the current cyber threat landscape, the College's cyber posture, and priority areas for governance, staff, and systems.

The following key sector-wide risks were noted:

- National and global cyber incidents continue to increase, impacting major organisations across sectors.
- The UK Government has issued correspondence to FTSE 350 CEOs in light of rising strategic cyber threats.
- The FE sector remains a significant target, with 86% of FE institutions reporting cyber attacks.
- Threat actors are increasingly accessing systems through compromised credentials ("logging in rather than hacking in").

Specific findings for the College were highlighted, including concerning results from the recent phishing exercise, indicating that human behaviour remains the highest-risk area. Risk ratings were assessed as red/black due to systemic vulnerabilities across distributed FE systems. Governance arrangements were considered strong but requiring enhanced focus on protection measures and staff training.

Technical and governance matters were discussed, including incident response arrangements and accountability. The College's continuity plans were acknowledged, and the need for a clearly defined authority structure for decisions relating to system shutdown was recognised. Consideration of a Security Operations Centre (SOC) model for improved detection and escalation was recommended.

Recommendations and next steps identified were as follows:

1. Strengthen mandatory cyber security training and ensure compliance monitoring.
2. Appoint a Governing Body Cyber Liaison Member to support escalation and communication.
3. Conduct cyber incident simulation exercises twice per year.

4. Review and, where appropriate, extend MFA and passwordless authentication options.
5. Explore the compartmentalisation of high-sensitivity data.
6. Continue development of recovery point and recovery time objectives (RPO/RTO).
7. Finalise the College's approach to mobile access and the segmentation of critical systems.

Members thanked BMC for the comprehensive presentation.

47.4 Internal Audit Cyber Security Report

The report was noted.

47.5 Date of Next Meeting

23 April 2026.

The meeting closed at 5.05pm.

Mr I Murphy, Chair _____ Date 26.03.26

Mrs K Wallace, Secretary _____