

**Glasgow Kelvin College**

**Finance and Resource Committee Meeting of 10 March 2026**

**ICT Security Policy**

**Report by Assistant Principal, Digital and Information Systems**

**1. Introduction**

The ICT Security Policy sets out the technical security principles and controls required to protect the confidentiality, integrity and availability of the College's digital systems and information. It provides clear direction for the secure design, operation and management of ICT infrastructure, supporting the College's wider Information Security Framework, data protection obligations, and acceptable use requirements.

The policy applies to all College-managed ICT systems, including on-premise and cloud services, and provides assurance to the Board that appropriate technical measures are in place to prevent, detect and respond to cyber security threats.

**2. Summary of Changes to the Policy**

The ICT Security Policy, provided at Appendix 1, has been reviewed to ensure it remains current, proportionate and aligned with relevant regulatory and best-practice frameworks. The review process included engagement with ICT staff, Senior Leadership Team and externally by HEFESTIS, who provide cyber security consultancy to the College. Key updates include:

- Alignment of the policy structure and controls to the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF), while maintaining consistency with the Scottish Public Sector Cyber Resilience Framework.
- Updates to reflect the College's increased use of cloud-hosted services and modern hybrid infrastructure, ensuring security requirements apply consistently across on-premise and cloud environments.
- Clarification of the policy's scope and its relationship to supporting policies and procedures, including the Information Security Framework and the ICT Incident Response Procedure.
- Minor revisions to terminology, structure and responsibilities to improve clarity, governance and auditability, with no change to the underlying intent of maintaining strong cyber security controls.

Overall, the review strengthens assurance that the College's technical security controls remain fit for purpose in a changing threat and technology landscape.

Amendments to the policy document are provided in yellow highlight.

### **3. Resource Implications**

No resource implications are identified as a consequence of this report.

### **4. Impact on students**

There are no issues identified that could impact students as a direct result of this report.

### **5. Equalities**

There are no equality implications arising directly from this report.

### **6. Risk and Assurance**

The review identifies no new material risks arising from the updated ICT Security Policy. The changes strengthen assurance by aligning controls with recognised cyber security frameworks and improving clarity of governance and responsibilities.

### **7. Data Protection**

No adverse data protection impacts have been identified. The revised policy reinforces existing technical safeguards and supports continued compliance with GDPR and the College's Information Security Framework.

### **8. Environmental and Sustainability**

There are no environmental and sustainability implications arising from this report.

### **9. Recommendations**

Members are recommended to:

- i note the content of this report and its appendices.
- ii endorse the ICT Security Policy.

### **10. Further Information**

Members can obtain additional information on the contents of this report from Jason Quinn, Assistant Principal, Digital and Information Services, [jquinn@glasgowkelvin.ac.uk](mailto:jquinn@glasgowkelvin.ac.uk).

Glasgow Kelvin College  
Jason Quinn, Assistant Principal, Digital and Information Services  
March 2026