

Glasgow Kelvin College
Board of Management Meeting of 10 June 2026
Using Copilot Safely and Securely
Report by Assistant Principal of Digital and Information Services

1. Introduction

The purpose of this report is to provide the Board with assurance on the College's use of Artificial Intelligence (AI), specifically in relation to the use of Microsoft 365 Copilot. This responds directly to questions raised by the Board regarding data security when using AI, particularly in the context of Board and Committee papers. The detailed assurance is provided in Appendix 1.

2. Key Position

The attached paper provides assurances that the use of Microsoft 365 Copilot within the College's Microsoft 365 environment operates within established security, data protection and governance controls. It concludes that, when used appropriately, this does not introduce a new or unmanaged risk.

3. Policy and Strategic Alignment

The assurance position aligns with the College's ICT Acceptable Use Policy and the Digital Enabler Framework, reinforcing that AI is to be used within approved systems and governed through existing information security and data protection arrangements.

4. Resource Implications

There are no direct resource implications arising from this report.

5. Impact on Students

There are no direct impacts on students arising from this report.

6. Risk and Assurance

The paper emphasises that risks associated with AI are primarily linked to information governance practices rather than the technology itself. The College continues to strengthen controls in this area through ongoing data protection and compliance activity.

7. Equality

No adverse impacts on individuals with protected characteristics have been identified.

8. Data Protection

The paper provides assurance that the use of AI is aligned with the College's data protection obligations and operates within established controls.

9. Environmental and Sustainability

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

10. Recommendations

It is recommended that members:

- i) note the content of the report within **Appendix 1**.

11. Further Information

Further information can be obtained from Jason Quinn, Assistant Principal, Digital and Information Services. at jquinn@glasgowkelvin.ac.uk

JQ
June 2026

Use of Artificial Intelligence (AI) and Data Security

Purpose

This paper has been prepared in response to a query raised by the Board regarding the security of using Artificial Intelligence (AI), particularly where Board or Committee papers containing confidential or sensitive information are used to generate executive summaries. The paper provides assurance on how the College is using AI safely, explains the controls in place, outlines associated risks, and clarifies where AI use is considered appropriate and where it would introduce unacceptable risk.

Background and Context

AI tools are now embedded across many mainstream productivity platforms. Within the College, the principal AI capability in use is Microsoft 365 Copilot, which is integrated into the existing Microsoft 365 environment used for email, documents, and collaboration. This is materially different from public, consumer AI tools that operate outside organisational control.

The concern raised by the Board related to whether uploading documents to an AI tool could result in data being stored or used outside the College's control. This concern is well-founded in the context of public AI tools. However, it is important to distinguish these from enterprise AI platforms that operate within contractual, technical, and regulatory safeguards.

How Microsoft 365 Copilot Works

Microsoft 365 Copilot does not function as a separate AI system where documents are uploaded or copied elsewhere. Instead, it operates within the College's Microsoft 365 tenancy, using the same security model that already applies to email, SharePoint and OneDrive documents.

When a user asks Copilot to summarise a document, the system temporarily reads the content only if the user already has permission to access it and uses that content to generate a response. This process is referred to by Microsoft as "grounding", meaning the AI is provided with context to answer a specific request. The document is not copied into a new database or made available to other users or organisations. Microsoft is explicit that data accessed in this way is not used to train AI models. However, Copilot interaction data, including user prompts, responses and supporting context, may be retained within Microsoft 365 for service, audit, security and compliance purposes, in line with Microsoft 365 logging, retention and eDiscovery controls. (Microsoft Learn, Data, Privacy, and Security for Microsoft 365 Copilot: <https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-privacy>).

Data Security and Confidentiality

Data Storage

College data held within Microsoft 365, including Copilot interaction data, is stored in line with the configured Microsoft 365 tenancy geography. The College's current data location is the United Kingdom, with commitments aligned to Microsoft's European data residency framework. As part of normal cloud service operation, some processing may occur across Microsoft's global infrastructure. However, this is carried out in accordance with Microsoft's enterprise data protection, security and compliance commitments (Microsoft Learn, Data Residency for Microsoft 365 Copilot:

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/m365-dr-service-copilot?view=o365-worldwide>).

Data in Transit

When Copilot accesses a document or generates a response, all data transfers are encrypted in transit using industry-standard transport encryption, in the same way as any other Microsoft 365 service. Microsoft confirms that Copilot data benefits from the same encryption and security controls as Exchange email and SharePoint documents (Microsoft Learn, Enterprise Data Protection in Microsoft 365 Copilot:

<https://learn.microsoft.com/en-us/microsoft-365/copilot/enterprise-data-protection>).

Access Controls

Copilot does not bypass security permissions. It can only access documents that the user is already authorised to open themselves. If a Board paper is restricted to Board members and Secretariat staff, Copilot cannot be used on that paper by anyone outside that group. This means responsibility for protecting sensitive content remains with existing information governance controls, not the AI itself (Microsoft Learn, Security for Microsoft 365 Copilot: <https://learn.microsoft.com/en-us/microsoft-365/copilot/security-microsoft-365-copilot>).

Use of AI with Board and Committee Papers

Where Board or Committee papers are finalised documents, stored within the College's Microsoft 365 environment and access is restricted appropriately, the use of Copilot to generate an executive summary or highlight key themes does not introduce a new category of data risk. In these circumstances, Copilot is performing a task that would otherwise be carried out manually by an authorised individual, using the same underlying information and subject to the same access controls.

The key expectation is that Board and Committee papers continue to be handled in line with existing confidentiality arrangements. This means papers should be created, stored and reviewed within controlled Microsoft 365 locations (such as SharePoint,

OneDrive or Word) where permissions, sensitivity labels and audit controls apply. When Copilot is used directly with documents in these locations, those protections remain fully in force.

Greater care is required where papers are still in draft form, contain particularly sensitive personal or commercial information, or where content is manually copied from a document into an AI chat interface. Copying content into chat does not result in the information leaving the College's Microsoft 365 environment, nor does it allow the information to be seen by external parties or used to train AI models. However, copying text into chat temporarily removes it from the original document's security context, meaning certain document-level safeguards, such as sensitivity labels, are no longer applied in the same way. For this reason, the preferred and safest approach for handling confidential Board material is to allow Copilot to work directly with the secured document wherever possible, and to limit copy-and-paste use to small, necessary excerpts only.

This distinction does not represent a security failure, but rather a matter of good information governance. By continuing to treat Board and Committee papers as confidential documents and using Copilot within the College's controlled Microsoft 365 environment, the College can benefit from AI-assisted summarisation while maintaining appropriate confidentiality and assurance.

Microsoft 365 Copilot is designed to support drafting, summarisation and analysis activities; however, it does not replace professional judgement or existing approval processes. All AI-generated outputs must be reviewed, validated and approved by the user before use in formal communications or decision-making. Responsibility for the accuracy and appropriateness of content remains with the author and approving officer.

Key Risks and Mitigations

The Board's concern regarding the use of AI is primarily centred on the potential for loss of confidentiality, inappropriate access to sensitive information, and uncontrolled onward sharing of College data. These risks are real in the context of public or consumer AI tools, but they are materially reduced when AI is used within the College's Microsoft 365 environment under established governance arrangements.

The principal risk is not the AI technology itself, but weaknesses in information governance. Over-permissive access to documents, inconsistent use of sensitivity labels, or poor handling of draft or confidential material can increase the likelihood that sensitive information is accessed more widely than intended. The introduction of AI can amplify the impact of such weaknesses by making information easier to summarise or analyse quickly.

This risk is mitigated through the College's existing controls. Board and Committee papers are held within secured Microsoft 365 locations, access is restricted to defined groups, and Copilot is technically unable to access content beyond a user's existing permissions. All data remains encrypted in transit and at rest, activity is logged for audit purposes, and Microsoft provides contractual assurances that College data is not reused, shared with other organisations, or used to train AI models. In addition, the College is implementing enhanced Microsoft Purview controls to further strengthen data protection, including measures to reduce the risk of data leakage and to address potential oversharing of content within Microsoft 365.

A secondary risk relates to user behaviour, particularly how sensitive content is introduced into AI chat interfaces. Where a file is uploaded into Microsoft 365 Copilot chat, the system explicitly stores a copy of that file in the user's OneDrive, where it retains the College's standard security controls, permissions, audit logging and tenancy isolation. No additional users gain access to that file unless it is explicitly shared. In contrast, where users manually copy and paste raw text into chat, the content remains visible only to the individual user and does not leave the College's environment, but it is temporarily detached from the original document's metadata. This means that certain document-level safeguards, such as sensitivity labels and automated policy enforcement, do not apply in the same way while the content exists as prompt text. The risk is therefore one of reduced automatic protection rather than wider access or disclosure, and it is mitigated through guidance that encourages staff to work directly with secured documents wherever possible and to apply proportional judgement when handling confidential material.

Taken together, these mitigations mean that the College's use of Microsoft 365 Copilot does not introduce unmanaged or unacceptable risk. Instead, it reinforces the importance of strong information governance practices that the College already applies.

Appropriate and Inappropriate Use

The College considers AI appropriate for tasks such as summarising lengthy reports, improving clarity of language, and supporting consistency in drafting, particularly where the user already has legitimate access to the content.

It is not appropriate to use AI tools outside the College's Microsoft 365 environment for College business, nor to input confidential, sensitive or personal information into public or consumer AI services unless explicitly authorised and subject to appropriate safeguards. These requirements align with the College's ICT Acceptable Use Policy and data protection obligations under GDPR.

Conclusion and Assurance

The College's use of Microsoft 365 Copilot operates within established Microsoft 365 security, governance and data protection controls, and is appropriate when used in line with existing information security and data protection arrangements.

The Board can therefore be assured that the use of Copilot to support activities such as generating executive summaries, when undertaken within the College's Microsoft 365 environment and with correct permissions in place, does not introduce a significant or unmanaged risk of data loss. This approach is consistent with the College's Digital Enabler Framework, which positions AI as a shared enabling capability delivered within secure, ethical and governance-led arrangements.