STEVENS
INSTITUTE OF TECHNOLOGY

Stevens Guide to Data Security and Protection in AI Tools

When using Artificial Intelligence (AI), ensure it aligns with Stevens' Information Security Policy, Privacy Policy, and any other relevant policies. Always consider the risks and ethical implications, and seek prior approval from your supervisor and/or department chair for new AI uses in your work.

Depending on the AI use case, additional consultation may be required. Key considerations include data sensitivity, regulatory compliance, ethical implications, user consent, data privacy, and intellectual property rights. These may necessitate consultation with the Office of Sponsored Projects, Office of the General Counsel, Division of Human Resources, Division of Information Technology, and/or the Office of Compliance.

Stevens Data Classification Standards and Appropriate Use of Artificial Intelligence

The Stevens Data Classification Standards can be used as a reference for potential use of AI. **These examples provide general guidance and are not exhaustive.**

Public This data is openly accessible and can be shared without restrictions.	**Non-Public** This data is not intended for public access but can be used internally within Stevens.	**Sensitive** This data requires careful handling and protection due to its potential impact if disclosed.	**Restricted** This data is highly confidential and its use is strictly controlled.
Permissible for AI Use	Use of Stevens data is **only permissible with licensed AI tools**, including Microsoft Copilot for Web with Data Protection and Zoom AI Companion, while logged in via a Stevens account.		**Prohibited** for AI Use
▪ Publicly available information ▪ Publications for general release ▪ Campus maps ▪ Course catalogs ▪ Public-facing web pages ▪ Job postings ▪ Public-facing recorded content	▪ Unpublished research data and other academic work that may be shared externally ▪ Administrative Publically available reports ▪ Data or information on Stevens infrastructure ▪ Lectures without student identifiers	▪ Financial data, records, and plans ▪ Meeting minutes and notes ▪ Lectures with student identifiers ▪ Sensitive research data and materials ▪ Data and reports that may only be shared internally ▪ Internal operational and administrative guidelines ▪ Internal analysis, draft status, or decision-making processes on sensitive data	▪ Any personally identifiable info ▪ Financial records ▪ Records and info subject to NDAs ▪ Research data which may only be shared internally ▪ Intellectual property or proprietary information ▪ Passwords ▪ Internal analysis, draft status, or decision-making processes on restricted data

Stevens Generative AI Overview contains several additional resources regarding AI. For questions regarding privacy, compliance, or security in the context of AI tools and their use contact Security@Stevens.edu.

Certain use cases, such as grading or assessment of student work, recruitment, personnel, or disciplinary decision-making, legal analysis or advice, security tools using facial recognition, and any non-public use of non-licensed AI tools with click-through agreements, requires additional review and consideration prior to use in AI.

For additional information or questions about data usage, please contact support@stevens.edu.