

Data Governance & Security

Keeping You Informed!

Guess who has a new website??

We're excited to announce the launch of Hamilton's new Data Governance website! This new hub brings together resources, policies, and guidance to help our community better understand how institutional data is managed, protected, and used responsibly across campus.

Whether you're looking to find out who our data stewards are, understand what a functional area is, access the data catalog, or request access to data, this site is designed to help you find what you need.



Explore the new site and learn how data governance supports a informed decision-making culture and protects the integrity of Hamilton's data assets.



Data Cookbook
Definitions

567



Data Cookbook
Users

125



Data Portal Dashboards

108

Byte-Sized Governance

- Who are our front line champions - [data stewards and data custodians](#) - that are protecting our data assets?
- [Data Governance Training](#) - Becoming a Data Champion and get a digital badge and a sticker!

- Hamilton College Data Citizenship Program (Coming Soon!)

Did you know-

LITS has a website to help the Hamilton College community understand and use artificial intelligence (AI)

Artificial Intelligence- Hamilton College



InfoSec Safety Dance Quick Tips

- **Beyond passwords:** Enable multi-factor authentication (MFA) on every account that supports it. A strong password is your first line — MFA is your safety net.
- **Think before you click:** Hover over links before opening them. If a sender or URL looks even slightly off, trust your instinct — verify through a separate channel before engaging.
- **Bots, breaches & malware — oh my:** Keep devices and software updated. Attackers actively exploit known vulnerabilities in unpatched systems. When IT pushes an update, apply it promptly.

ACTIVE IMPROVEMENT

Proactive phishing removal coming to Hamilton inboxes

Information Security is working to proactively identify and remove phishing emails from Hamilton inboxes before you ever see them. In the last three months alone, over 16 million email messages were sent and received by Hamilton — and more than 40,000 of those were phishing attempts.

The most impersonated Person? Our very own Steven Tepper. Always verify the sender's identity and confirm you have a valid email address before responding to any unexpected message.

WATCH OUT!

ListServ approval requests you didn't originate.

A common tactic used by malicious actors is to send ListServ approval requests to a valid Hamilton inbox. If you receive an approval request for a message you did not submit, **do not approve it**. Approving it sends that message to the entire list —don't be an unwitting assistant to a spammer.

CALENDAR PHISHING

Uninvited Google Calendar events appearing in your calendar?

A growing phishing trend involves attackers sending Google Calendar invites that automatically appear in your calendar — even without your consent. You can stop this by changing one setting.

In Google Calendar settings, set "**Add invitations to my calendar**" to "**Only if the sender is known.**" This prevents unsolicited events from appearing automatically.

KNOW BEFORE YOU GO

Using AI tools? Keep these principles in mind.

AI tools can be powerful — but what you put in matters. Avoid entering sensitive institutional data, student information, or personal details into AI systems not approved for that purpose.

And always keep a human in the loop: AI output should be reviewed, not blindly trusted.

– [Review Hamilton's Generative AI Guidelines](#)

Library and Information Technology Data Governance & Security
hamilton.edu/data-governance

Hamilton College | 198 College Hill Rd | Clinton, NY 13323 US

[Unsubscribe](#) | [Constant Contact Data Notice](#)