Preliminary Guidelines for the Use of Generative AI Tools by the Idaho State University Community

Generative artificial intelligence (AI) tools are rapidly advancing and have the ability to change how we teach, learn and work. As an institution dedicated to the development and dissemination of knowledge, Idaho State University (ISU) recognizes the importance of this new technology. ISU also recognizes the necessity of ensuring that use of generative AI honors our existing commitments to security and privacy and our values as expressed through ISU Policies and Procedures. A taskforce of administrators and faculty from various parts of the University has been created to guide the responsible use of AI tools at ISU. As AI technology evolves, so will these guidelines.

The following are areas of particular concern:

1. **Confidentiality**: Many generative AI tools incorporate all information entered by users into their model. ISU community members must not enter information requiring confidentiality into an AI tool without ensuring information entered will be protected from redisclosure or use in responses to others, as documented by appropriate contract language and security controls. When in doubt, do not enter any confidential information into an AI tool.

2. **Protection of PII**: Because many AI tools use the information you include in them, always assume that anything you input will become public. Never include protected personal information such as patient records, student education records, or any other information which should be maintained as private. Be mindful of the application of laws such as HIPAA and FERPA, which have strict requirements for how personal PII is to be maintained.

3. **Transparency:** Be transparent in your use of AI tools and always disclose when your work includes information acquired through the use of an AI tool.

4. **Academic Integrity**: Faculty should make clear to students whether use of AI tools is permitted and, if so, whether there are limits or restrictions on such use. Students should ask faculty whether use is permitted if clear authorization has not been provided. If AI tools are used, attribution should be given to ensure that work submitted properly credits sources of information.

5. **Intellectual Property Rights**: Generative AI may use information that is protected by intellectual property rights, including copyrighted materials, without consent or other appropriate authorization. Users should be cautious not to expose themselves or the University to claims of damage from third parties for improper use of other's work. Users should also be aware that by including their own original work into an AI tool, they may risk losing protection of their own intellectual property rights or that of the University. University owned intellectual property may not be put into a generative AI tool.

6. **Protection of ISU Data**: Do not enter any ISU protected data or information into an AI tool.

7. **Bias and Inaccuracy**: Reports that AI generated responses are biased or inaccurate are common. Be a critical thinker and verify information provided by an AI tool prior to incorporating it into your work.

8. **Procurement**: As is the case when acquiring any technological product which will be using University resources or University data, consult with Information Technology Services and follow ISU's purchasing policies. AI tools should not be acquired until the security of the tool has been validated and the appropriate University offices have verified inclusion of contract language appropriately protecting the University.

9. **Malicious Content**: Generative AI tools may create avenues for improper access to ISU's information technology system. All members of the ISU community are responsible for protection of ISU's information technology system. Be alert. As with any technological resource, use it responsibly.

When using Generative AI tools, be mindful that all use must comply with the ISU Policies and Procedures which govern our community, including those concerning data privacy and confidentiality, academic integrity, human resources, information security and procurement. www.isu.edu/policy/. The following list includes potentially applicable policies:

- Contract Approval and Execution ISUPP 1060
- Electronic and Information Technology Accessibility ISUPP 1020
- Equal Opportunity, Harassment and Non-discrimination ISUPP 3100
- HIPAA Compliance ISUPP 1100
- Purchasing ISUPP 2560
- Equal Opportunity and Affirmative Action ISUPP 3080
- Academic Freedom ISUPP 4040
- Academic Integrity and Dishonesty ISUPP 4000
- Faculty Ethics ISUPP 4120
- Student Code of Conduct ISUPP 5000
- Intellectual Property ISUPP 7010
- ISU Export Controls ISUPP 7040
- ITS Acceptable Use ISUPP 2400
- ITS Access Control ISUPP 2410
- ITS Acquisitions, Development and Maintenance ISUPP 2420
- ITS Asset Management ISUPP 2430
- ITS Information Security ISUPP 2500
- ITS Security Roles and Responsibilities ISUPP 2480