Terms of use

THESE TERMS OF USE FORM A BINDING CONTRACT BETWEEN ASU PREP DIGITAL (ASUPD), ON BEHALF OF ITSELF AND ASU PREP ACADEMY AND ASU PREP GLOBAL AND YOU. BY USING ASU’S COMPUTING, INTERNET, AND COMMUNICATION RESOURCES, YOU AGREE TO BE BOUND BY THESE TERMS OF USE.

A. Background

These Terms of Use apply to all uses and users (Users) of ASUPD’s computing, Internet, and communication resources (ASUPD Computing and Communication Resources). ASUPD Computing and Communication Resources include ASUPD’s websites and information posted thereon, software and online services provided by ASUPD, including through the cloud, and ASUPD’s technology network, ASUPD’s and its authorized third parties’ curriculum and communications and computing devices. ASUPD Computing and Communication Resources also include computers, data storage systems, mobile devices, electronic data, networks, electronic mail services, electronic information sources, voice mail, telephone services, and other communication resources.

In addition, these Terms of Use reflect the goal of ASUPD to foster academic freedom while respecting the principles of freedom of speech and the privacy rights of Users.

ASUPD Computing and Communication Resources are the property of ASUPD. They are to be used for the advancement of ASUPD’s educational, research, service, community outreach, administrative, and business purposes. ASUPD’s Computing and Communication Resources are provided for the use of faculty, staff, currently admitted or enrolled students, and other properly authorized Users. ASUPD may, at its discretion, permit Users to have the access to accounts and e-mail forwarded or redirected for a limited period of time.

The University Technology Office (UTO) is responsible for the maintenance and security of ASUPD’s central computing and communications resources. This includes recommendations for effective practices by its Users, These Terms of Use are designed to aid the ASUPD community in protecting the confidentiality, availability, and integrity of ASUPD Computing and Communication Resources. ASUPD owns and maintains all of its proprietary curriculum and
related content including, but not limited to, instructor resources, test banks and other materials necessary to effectively conduct virtual classes. ASUPD is responsible for the maintenance and updating of all proprietary curriculum and related content.

All uses and Users of ASUPD Computing and Communication Resources must comply with these Terms of Use, as well as ASUPD’s Privacy Statement and ASU’s Computer, Internet, and Electronic Communications Information Management Policy. All uses of ASUPD Computing and Communication Resources must also be consistent with ASU’s Charter and Mission.

We encourage you to periodically review these Terms of Use because ASUPD may update them from time to time.

B. Requirements for Use of ASUPD Computing and Communication Resources

1. You must comply with all applicable local, state, and federal laws and regulations, and with ASUPD and Arizona Board of Regents (ABOR) policies.
2. You must respect academic freedom and free speech rights.
3. You must be truthful and accurate in personal and computer identification.
4. You must respect the rights and privacy of others, including intellectual property and personal property rights.
5. You must not compromise the integrity of electronic networks, must avoid restricted areas, and must refrain from activities that may damage ASUPD Computing and Communication Resources, and transmitted or stored data.
6. You must maintain the security of accounts and must protect and regularly change their account passwords according to standards maintained by UTO.
7. You, once aware of a security concern, must notify ASUPD at asuprepinfosec@asu.edu of information security concerns including, but not limited to, breaches of sensitive data or compromised accounts.
8. You are responsible for the protection, security, and integrity of ASUPD data and resources under your control according to the standards maintained by UTO. See the ASU Information Security Standards for more information.

C. Prohibited Uses of ASUPD Computing and Communications Resources

1. Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications, are prohibited.
2. Use of ASUPD Computing and Communication Resources for private business or commercial activities, or for fund-raising or advertising on behalf of non-ASUPD organizations, is prohibited.
3. The unauthorized reselling of ASUPD Computing and Communication Resources is prohibited.
4. Unauthorized use of ASUPD’s trademarks or logos and other protected trademarks and logos is prohibited.
5. Any alteration of addresses, uniform resource locator (URL), or other action that masks the asuprepdigital.org domain as a host site is prohibited unless authorized by UTO.
6. Unauthorized anonymous and/or pseudonymous communications are prohibited. All Users must cooperate with appropriate ASUPD personnel or other authorized personnel when investigating the source of anonymous messages.
7. Misrepresenting or forging the identity of the sender or the source of an electronic communication is prohibited.
8. Unauthorized attempts to acquire and use passwords of others are prohibited.
9. Unauthorized use and attempts to use the computer accounts of others are prohibited.
10. Altering the content of a message originating from another person or computer with intent to deceive is prohibited.
11. Unauthorized modification or deletion of another person’s files, account, or news group postings is prohibited.
12. Use of ASUPD Computing and Communication Resources or data without authorization or beyond one’s level of authorization is prohibited.
13. Interception or attempted interception of communications by parties not authorized or intended to receive them is prohibited.
14. Making ASUPD computing resources available to individuals not affiliated with ASUPD without approval of an authorized ASUPD official at or above the level of dean/university librarian or director is prohibited.
15. Compromising the privacy or security of electronic information is prohibited.
16. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction) is prohibited. The unauthorized storing, copying, or use of audio files, images, graphics, computer software, data sets, bibliographic records, and other protected property is prohibited except as permitted by law.
17. Interference with or disruption of the computer or network accounts, services, or equipment of others is prohibited.
18. The propagation of computer “worms” and “viruses,” the sending of electronic chain mail, denial of service attacks, and inappropriate “broadcasting” of messages to large numbers of individuals or hosts are prohibited.
19. Failure to comply with requests from appropriate ASUPD officials to discontinue activities that threaten the operation or integrity of computers, systems, or networks, or that otherwise violate these Terms of Use is prohibited.
20. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access without authorization is prohibited.

21. Altering or attempting to alter files or systems without authorization is prohibited.

22. Scanning of networks, networked devices, or applications for security vulnerabilities without specific authorization by UTO is prohibited.

23. Attempting to alter or connect any computing or networking components (including, but not limited to, bridges, routers, DHCP servers, wireless access points, and hubs) on ASU’s technology network without approval of UTO is prohibited.

24. Installation or alteration of wiring, including attempts to create network connections, or any extension or retransmission of any computer or network services without the approval of UTO is prohibited.

25. Conduct leading to disruption of electronic networks or information systems is prohibited.

26. Conduct leading to the damage of ASUPD electronic information/data, or ASUPD Computing and Communication Resources is prohibited.

D. Prohibited Access

ASUPD may restrict access from within its network to any sites in furtherance of these Terms of Use. You may contact ASUPD at asuprepinfosec@asu.edu to request access to a restricted site or to report that a site was restricted in error. ASUPD may restrict you from accessing ASUPD Computing and Communication Resources.

E. Information Posted to ASUPD Computers or Web Pages

1. Restriction on Use of ASUPD Web Pages
   ASUPD’s website and web pages may be used only for ASUPD business and only authorized individuals may modify or post materials to these pages. No other pages may suggest that they are ASUPD web pages. If confusion is possible, pages should contain a disclaimer and links to ASUPD sites.

2. Responsibilities of Individuals Posting Materials
   By posting materials and using ASUPD Computing and Communication Resources, each User represents that he or she has created the materials or that he or she has the right to post or use the materials. The storage, posting, or transmission of materials must not violate the rights of any third person in the materials, including copyright, trademark,
patent, trade secrets, and any rights of publicity or privacy of any person. Materials posted must not be defamatory, libelous, slanderous, or obscene.

3. **Prohibition against Commercial Use**
   ASUPD Computing and Communication Resources may not be used for unauthorized commercial purposes.

4. **Control of ASU Web Pages**
The use of ASUPD Computing and Communications Resources, including ASUPD’s website is at the sole discretion of ASUPD. ASUPD does not guarantee that any User will have continued or uninterrupted access to ASUPD’s website. ASUPD’s website may be removed or discontinued at any time at the discretion of ASUPD in accordance with ASUPD policy, or as needed to maintain the continued operation or integrity of ASUPD Computing and Communication Resources.

ASUPD makes reasonable efforts to protect the integrity of its technology network and related services, but ASUPD cannot guarantee backup, disaster recovery, or User access to information posted on web pages or personal computers.

**F. Electronic Mail and Electronic Communications**

1. **Conditions for Restriction of Access to Electronic Mail**
Access to ASUPD e-mail is a privilege that may be wholly or partially restricted without prior notice and without consent of the User:

   a) If required by applicable law or policy;

   b) If a reasonable suspicion exists that there has been or may be a violation of law, regulation, or policy; or

   c) If required to protect the integrity or operation of ASUPD’s e-mail system or Computing and Communication Resources or when ASUPD Computing and
Communication Resources are required for more critical tasks, as determined by appropriate management authority.

Access to ASUPD’s e-mail system may require approval of the appropriate ASUPD supervisory or management authority (e.g., department head, system administrator, etc.).

2. **Conditions for Permitting Inspection, Monitoring, or Disclosure**

ASUPD may permit the inspection, monitoring, or disclosure of e-mail, computer files, and network transmissions when:

a) Required or permitted by law, (including public records laws), subpoenas, or court orders;

b) ASUPD or its designated agent reasonably believes that a violation of law or policy has occurred; or

c) Necessary to monitor and preserve the functioning and integrity of the e-mail system or ASUPD Computing and Communications Resources.

You must cooperate and comply with ASUPD requests for access to and copies of e-mail messages or data when access or disclosure is authorized by these Terms of Use or required or allowed by law or other applicable policies.

3. **ASUPD Responsibility to Inform of Unauthorized Access or Disclosure**

If ASUPD believes unauthorized access to or disclosure of information has occurred or will occur, ASUPD will make reasonable efforts to inform the affected computer account holder, except when notification is impractical or when notification would be detrimental to an investigation of a violation of law or policy.

4. **Prohibition against Activities Placing Strain on ASUPD Computing and Communication Resources**

Activities that may strain ASUPD’s e-mail or Computing and Communication Resources more than can be reasonably expected are in violation of these Terms of Use. These
activities include, but are not limited to: sending chain letters; “spam,” or the widespread dissemination of unsolicited e-mail; and “letter bombs” to resend the same e-mail repeatedly to one or more recipients.

5. **Confidentiality**
Confidentiality of e-mail and other network transmissions cannot be assured. Therefore, you must exercise caution when sending personal, financial, confidential, or sensitive information by e-mail or via ASUPD Computing and Communications Resources.

6. **Electronic Information as Arizona Public Record**
Most electronic information (e.g., e-mail) produced in the course of ASUPD business is considered an Arizona public record, and must be stored or deleted in accordance with [Arizona public records law](#). Consult with ASUPD’s archivist for guidance on procedures for external storage or deletion of public records.

G. Privacy and Security

1. **Routine Logging and Monitoring**
Certain central service and network activities from workstations connected to the network are routinely logged and monitored. These activities include but are not limited to:

   a) Use of passwords and accounts accessed;

   b) Time and duration of network activity;

   c) Access to Web pages;

   d) Access to network software;

   e) Volume of data storage and transfers; and

   f) Server space used for e-mail.

2. **Detailed Session Logging**
In cases of suspected violations of ASUPD policies, especially unauthorized access to ASUPD Computing and Communication Resources, the appropriate system administrator, after consultation with ASUPD offices, may authorize detailed session logging. This may involve a complete keystroke log of an entire session. In addition, the system administrator of the facility concerned may authorize limited searching of User files to gather evidence on a suspected violation.

3. **Responsibility for Data Security**
Software and physical limitations, computer viruses, and third-party intrusions can compromise security of data storage and communications. ASUPD takes reasonable precautions to minimize risk.

ASUPD Computing and Communication Resources are managed by ASUPD departments, or UTO, depending on a variety of business factors. UTO is not obligated to maintain backups of any file for any particular length of time. Users must protect and back up critical data.

4. **Restriction of Access to Sensitive Data**
All ASUPD departments should ensure that access to sensitive data is restricted to those employees who have a need to access the information. Passwords that provide access to sensitive information should be changed on a regular basis.

5. **Right to Examine Computing and Communication Resources**
ASUPD Computing and Communication Resources may be examined to detect illegal content, to evaluate the security of the network, and to detect violations of Arizona Board of Regents and ASUPD policies. Networks, networked devices, and applications may be scanned for vulnerabilities as authorized by UTO.

H. **Violations and Enforcement**

1. **Reporting Violations**
Any actual or suspected violation of these Terms of Use should be brought to the ASUPD system administrator of the equipment or facility most directly involved. In the
case of a serious violation, Users are required to make a report to ASU’s Information Security Office.

2. **ASUPD Response to a Reported Violation**
   Upon receiving notice of a violation, ASUPD may temporarily suspend your privileges, move, or delete the allegedly offending material pending further proceedings.

   A User accused of a violation will be notified of the charge and have an opportunity to respond before ASUPD imposes a permanent sanction. Appropriate cases will be referred to the ASUPD disciplinary authority appropriate to the violator’s status or to appropriate law enforcement authorities.

   In addition to sanctions available under applicable law and ASUPD and ABOR policies, ASUPD may impose a temporary or permanent reduction or elimination of access privileges to ASUPD Computing and Communication Resources, and other services or facilities.

   If ASUPD believes it necessary to preserve the integrity of Computing and Communication Resources or data, ASUPD may temporarily suspend any account, whether or not the account User is suspected of any violation. ASUPD will provide appropriate notice to the User. Servers and computers that threaten the security of ASUPD Computing and Communication Resources will be removed from the network and allowed to reconnect only with the approval of UTO.

3. **Indemnification by Users**
   Unless you are an ASUPD employee acting within the course and scope of your employment with ASUPD, you agree to indemnify, defend, save and hold harmless the State of Arizona, its departments, agencies, boards, commissions, universities, and its and their officials, agents and employees for, from, and against any and all claims, actions, liabilities, damages, losses, or expenses (including court costs, attorneys’ fees, and costs of claim processing, investigation, and litigation) for bodily injury or personal injury (including death), or loss or damage to tangible or intangible property to the extent caused, or alleged to be caused, by (i) the User’s negligence, acts or omissions; (ii) a breach of these Terms of Use; or (iii) failure to comply with any applicable law. You will
be responsible for primary loss investigation, defense and judgment costs where this indemnification is applicable.

I. Contact

For questions regarding these Terms of Use, please contact ASUPD at https://contact.asu.edu/.