DAVIDSON COLLEGE

Davidson College Technology Terms of Service

Davidson College Technology Terms of Service

Background

These Terms of Service ("Terms") apply to all individuals ("End Users") using Davidson College's network, technology services, computing equipment, telecommunications systems, and other technology or communications platforms ("Services"). Unless otherwise stated, the Terms apply to all Davidson College ("Davidson") End Users and Services.

Purpose

These Terms summarize the expected and appropriate use of Davidson Services. In some cases the Terms reference other applicable Davidson policies. End Users must comply with all applicable Davidson codes of conduct and policies when using the Services, including any Davidson policies not referenced here.

By using Davidson Services, End Users agree to these Terms, including the policies referenced herein.

If you have questions about these Terms, contact the Davidson Technology & Innovation (T&I) Support Center (704-894-2900, ti@davidson.edu, support.ti.davidson.edu).

Policy

Terms for All End Users

1) **Purpose of Services:** All Services are intended for academic, administrative, and non-commercial purposes related to the mission, objectives, and operations of Davidson College. Accordingly, End Users should use Davidson Services in a manner appropriate for their intended use and in accordance with the College's Statement of Purpose.

2) **Requesting Exceptions to the Terms:** These Terms include restrictions on the uses of Services to ensure that all Services are available for all End Users to the greatest extent possible. However, Davidson's teaching, learning and research mission may from time to time contemplate uses of Services that would not comply with these Terms. Davidson T&I is committed to working with End Users to find alternative means of supporting such needs wherever possible. End Users concerned about a conflict between their desired uses of Services and these Terms should contact the T&I Support Center in advance to discuss any needed exceptions to these Terms or other policies.

3) **Inappropriate Use of Services Prohibited**: End Users must not use Davidson Services:

- For unethical, illegal or criminal purposes;
- For personal economic gain or unauthorized commercial purposes;

- In any manner that violates Davidson's codes of conduct or policies, including those on discrimination and harassment.

4) **Examples of Inappropriate Use of Services**: Inappropriate uses of Services include, but are not limited to:

- Creating, viewing, publishing, transmitting, recording, or storing any content or data that violates federal, state or local laws;
- Sending deceptive and false emails or electronic communications, or engaging in activities to defraud or trick someone;
- Sending "spam," chain letters, or any other type of unauthorized widespread distribution of unsolicited email (see Davidson's guidelines on sending mass emails);
- For employees, using Davidson Services to support or oppose any candidate, party, or issue in an election for office or party nominations (see Davidson's policy on political activity in the Employee Guide);
- Accessing, deleting, or modifying content including files and information to which the End User is not authorized;
- Gaining unauthorized access to or interfering with the operation of Davidson Services;
- Interfering with the normal and reasonable use of Davidson Services by others whether via Davidson-owned or personally-owned devices;
- Using Davidson services (such as Davidson's network or computers) to gain unauthorized access to or interfering with non-Davidson IT systems, websites and other Internet-accessible resources;
- Except where explicitly authorized by T&I, probing or scanning Davidson Services for security vulnerabilities or taking actions that may compromise the data or privacy of others (such as network packet captures) without the explicit authorization of T&I (see Section 11 below for more information);
- Copying or stealing computer software or proprietary information, or violating the copyrights of others (for more information, see the College Copyright Policy and guidelines);
- Deliberately altering or damaging Davidson Services, Davidson-owned devices, or the personally-owned devices of others.

5) **Limited Personal Use Permitted**: Reasonable personal use of Davidson-owned Services (such as computers and phones) with the approval of an employee's supervisor is permitted, as long as it is performed in a safe, secure manner that otherwise complies with these Terms and other College policies.

6) **Services Ownership and Privacy Expectations:** Content on the Services may include Davidson-owned information (like college records and data) as well as information Davidson does not own (like student course submissions or content subject to the Davidson Intellectual Property Policy). In either case, Davidson Services are owned, operated and controlled by the College, and authorized staff including authorized third-party service providers may inspect and monitor Services including their content when necessary to responsibly manage and secure the Services or in response to authorized requests.

- Davidson staff do not routinely inspect the content of emails, files and other content on the Services, but as the owner and operator of the Services, Davidson does reserve the right to do so without advance notice to or the consent of End Users. End Users should have no expectation that any information created, transmitted, recorded, stored or posted on the Services will remain private.
- Davidson implements and uses automated security services to detect and block Internet sites, email messages, and other content that are known or likely to contain malware or other information security threats.
- Davidson maintains activity logs on Davidson Services in accordance with technology and security best practices. (See the Log Retention Guidelines for details.)
- For more details, see the College Access to Electronic Communications Policy.

7) **End User Credentials**: Access to most Davidson Services requires a username/email address and multiple security factors (such as a password and a cell phone or security key). End Users may never post or share their credentials with other persons, including parents and family members, and must contact Davidson's T&I Support Center if they believe their account or credentials have been lost, stolen or compromised. Some Services are available to college guests or parents using separate login methods.

- Davidson staff may temporarily suspend End User accounts, devices or access to Services if we suspect or detect evidence of password or account compromise or other threats to the security of our Services.

8) **Security and Configuration of Connected Devices**: Davidson provides network, internet and related telecommunications services to End Users, including to Davidson-owned devices assigned to or used by them, and to End Users' personal devices. Devices should be connected to the appropriate wireless or wired network for that type of device.

- Davidson-owned devices are managed and secured by authorized Davidson staff. End Users are not permitted to disable, circumvent or change security and management settings on these devices.
- End Users may connect allowed personally-owned devices to network services, and are responsible for ensuring the devices have the latest security updates provided by the manufacturer or software vendor and, where appropriate, updated anti-virus and security software.
- End Users may not connect devices running end-of-life, unsupported, or insecure software to the Davidson network or Services. Davidson may disconnect or deny network access and other Services to such devices.
- Some devices may never be connected to the Davidson network, or connected only with permission. Consult the Davidson Technology Purchasing Guide (Davidson login required) or contact the T&I Support Center for more information.
- While Davidson staff make every effort to deliver network services that are secure, Davidson cannot guarantee that malicious users or other parties are unable to intercept electronic communications. All users of network services should use secure, encrypted protocols and technologies for communications and applications, particularly those where End Users or Davidson are at risk if communications are breached or intercepted.

9) **Telecommunications Services**: Davidson is not responsible for cellular/mobile phone connectivity services provided by cell phone providers, and End Users should be aware that there is no guarantee of uninterrupted coverage on campus. Areas of no cellular coverage may exist in some places. Davidson recommends that End Users enable "WiFi calling" or equivalent features on their mobile phone if supported by the carrier. End Users are responsible for ensuring that they register an E911 location/address with their carrier as required.

- Employees who are issued a campus telephone number and/or desk phone are responsible for updating their E911 location when they change office/work locations by contacting the T&I Support Center or updating their location in the phone system through self-service means, if available.

- Davidson reserves the right to contact End Users by phone, SMS or similar methods to verify or restore End User access to Services or for other operational purposes as appropriate.

10) **Personal and Departmental Internet/Web Services and Domain Names**: Davidson provides web hosting services for personal identity and other types of content. The End User requesting such services, or their department, is responsible for ensuring these services comply with the Terms.

- Any subdomain of davidson.edu (such as somesite.davidson.edu) or any domain name that implies a Davidson affiliation (such as somedavidsondepartment.org) must be approved by College Communications or their designee.
- All publicly accessible websites affiliated with or linked to by the college must comply with Davidson policies on accessibility. (See the Web Accessibility policy.)
- All websites or Internet-facing services affiliated with or hosted by the college must be hosted in a location approved by T&I. The developer of the website/service is responsible for the effort and costs to update the site over time, including ensuring that security vulnerabilities are addressed in a timely fashion to T&I standards, and addressing end-of-life or obsolete technologies.
- Restricted or Confidential data as classified in the Data Security Policy may not be hosted on personal/departmental Internet services or websites without the explicit permission of T&I.
- Sites and services that do not meet these requirements may be limited to on-campus use only or disabled, as appropriate.

11) **Reporting Security Issues or Malicious Content**: End Users who receive a potentially malicious or dangerous email (such as one seeking to steal Davidson credentials) or emails or other content containing viruses or malware should immediately report the event to the T&I Support Center. End Users who encounter a vulnerability or security issue in a Davidson Service must cease using the Service immediately and contact the Support Center. Abuse or exploitation of vulnerabilities on Davidson Services is explicitly prohibited.

12) **Compliance with Export Control Laws**: Davidson provides Services primarily for our operation as a residential liberal arts campus. Students, faculty and staff who access Services outside the United States or transport College-owned technology equipment internationally are responsible for understanding and complying with export and import regulations, including those that prohibit

transporting or using encryption or other regulated technologies in prohibited countries. Contact the College's office of general counsel for more information.

13) **Non-Compliance with These Terms**: Davidson may temporarily or permanently suspend End User access to some or all Services for actual or potential violations of these Terms or other Davidson policies, or as required by law. End Users in violation of these Terms or Davidson policy may also be subject to further disciplinary action by Davidson College and/or the Honor Council, as well as legal action by the proper authorities where violations of state or federal law are involved.

Additional Terms for Davidson Employees (Including Student-Employees)

The following Terms apply to Davidson faculty, staff, contractors and other employees, including student-employees in their employment capacity.

14) **Responsibility for the Security of Davidson Information**: Information, data and other content that is owned by Davidson is intended solely for the authorized use of employees to conduct Davidson business. All employees are responsible for ensuring they are accessing, using and storing data in accordance with Davidson policy.

- Some Davidson information is protected by law, regulation, contract, or Davidson policy in ways that restrict its use, access, download and sharing.
- All employees who may access or create non-public information or information about persons other than themselves are expected to read, understand and comply with the Data Security Policy and Data Privacy Statement.
- Davidson employees with access to Restricted and Confidential information as defined in the Data Security Policy must transmit and store such data only on approved, encrypted Services and encrypted Davidson-managed devices only; may not store such data on personally-owned devices; and should use additional security such as encryption or VPN when transferring or accessing such information over public networks;

- All employees or students who are responsible for maintaining or managing information systems (including IT systems, servers, applications or other technology services that use Davidson Services including hosting and the campus network) are expected to read, understand and comply with the Information Systems Security Policy.

15) **Responsibility for the Security of Davidson Services including Computers/Devices**: All employees with access to Davidson Services are responsible for exercising appropriate caution and following best practices to ensure the security of such Services, including but not limited to any laptop, desktop or other computer issued to them. This includes:

- Physically securing computers and devices, including securing one's workspace and taking special care with portable devices to avoid their theft or loss;
- Returning any devices or removable media to T&I when no longer needed or at end of employment to ensure it is securely erased or destroyed in accordance with Davidson standards;
- Accepting and installing operating system, software and other updates on devices and other Services in a timely manner to minimize security vulnerabilities and protect device and Services from compromise;
- Not circumventing any cybersecurity and backup software implemented by T&I on devices and Services;
- Requesting approval from T&I before implementing any technologies allowing devices on the campus network or other Services to be accessed from outside the campus network (e.g. remote control software);
- Logging off Services and devices when no longer in active use, and locking devices when stepping away from an office or workspace so that others may not access them;
- Reporting any security concerns in a Service or device in a timely fashion.

16) **College Purchases of Technology**: T&I is responsible for all technology purchases at Davidson.

- All Davidson-owned technology devices (including computers, servers, tablets, research equipment, etc.) must be purchased by Davidson T&I regardless of funding source, and must be returned to Davidson at the end of its service lifespan or when its assigned End User is no longer affiliated with Davidson. For more details, see the Computer Workstation Purchasing policy.

- All other Services (including software applications hosted at Davidson as well as IT services provided and hosted by a third-party or vendor) must be reviewed and approved by T&I. No contract involving technology may be signed without review of the Chief Information Officer or their designee. For more details, see the Davidson Technology Purchasing Guide.

17) **Termination of Access Upon Departure**: All access to Davidson Services ordinarily ends automatically following the end of a faculty or staff appointment at the college. Accounts are deactivated and later deleted according to an automated schedule based on role and date

of departure; contact the T&I Support Center for details. It is the responsibility of departing faculty and staff and their supervisors to arrange the orderly transition of files, emails and other content from the employee's account for ongoing departmental or college use. The College Access to Electronic Communications Policy (requires Davidson login) also provides for supervisors, managers and department chairs to access departed employees' files and other content before account deletion if required.

- Faculty who are granted emeriti status may be eligible to retain access to select Services including their email account and a computer. During the transition to the applicable emeriti status, the faculty member must work with T&I to ensure that any confidential College data are transferred securely or erased and no longer accessible, and any College software is removed from computers that are used off campus. Additionally, any technology products or services (such as websites, apps or other services) developed or maintained by retiring faculty should be transitioned to another responsible faculty member or department for ongoing maintenance, or should be archived during the transition process.
- Managers who wish to maintain departing employees' access beyond their last day worked may request guest access, but should contact Human Resources to ensure that any needed contractor agreements, non-disclosure agreements, etc. have been signed.

18) **Guest Access**: Authorized End Users may request access for guests, contractors, vendors and others requiring credentials to access Davidson Services. The End User who approves and sponsors such access ("Sponsor") is responsible for ensuring that Sponsored Guests comply with all Davidson policies including these Terms, and for terminating credentials and all access to Services when no longer needed.

19) **No Unauthorized Third Party Disclosure**: Employees receiving subpoenas, legal demand letters, law enforcement requests, or other inquiries for data or information from Davidson Services may take no action on such requests without the approval of their division head and/or General Counsel.

Administration of Policy

The CIO shall oversee this policy and review it at least once every two years. Changes to this policy shall be made in accordance with the college's Policy on Policies.

Last Revised: April 2022