Hebrew College Acceptable Use of Information Technology Resources

Responsible office	CIT – Center for Information Technology team
Responsible party	Director of information technology
Last Save Date	12/22/2025
Status	Draft – awaiting approval or suggested edits
Last revision	12/22/2025
Approved by	Data Management Group
Approval date	9/3/20
Effective date	9/3/20
Last review	12/22/2025

Contents

1. Overview & Purpose

Information Technology resources are provided to Hebrew College faculty and staff as tools to facilitate the educational mission and business activities of the College. The purpose of this policy is to outline the acceptable uses of computer assets, applications/data, and communication systems at Hebrew College. Internet/Intranet/Extranet-related systems including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, and Internet browsing, and File Transfer Protocol, also known as FTP, are the property of Hebrew College. These systems are to be used for business purposes in serving the interests of the company and of our constituents, in the course of normal business operations. These rules are in place to protect employees and Hebrew College. Inappropriate use exposes Hebrew College to significant risks including, but not limited to, virus or malware attacks, compromised network systems and services, and legal issues. Compliance with this policy is a condition of continued employment by Hebrew College.

1.1. Disclaimer

The use of these resources is a privilege and is nontransferable. It is intended solely for the administrative and educational purposes of the community. These privileges are only made available to matriculating students registered for Hebrew College courses, faculty and staff. Public Internet access for research purposes is also available in the library.

Hebrew College reserves the right to change its usage policy and procedures at any time, including setting limits or prohibiting access. Hebrew College's computer services are administered by the Information Technology Department under the direction of Chief Financial and Administrative Officer.

2. SCOPE

This policy applies to employees, contractors, consultants, volunteers, and other workers at Hebrew College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Hebrew College. This policy applies to anyone with access to the assets, systems, and services this policy governs.

3. POLICY DEFINITIONS

Assets are all physical and digital technology resources owned, leased, or managed by Hebrew College. This includes desktops, laptops, smartphones, tablets, servers, printers, and any other devices capable of accessing the College's networks and systems.

Bandwidth is the transmission capacity of an electronic communications device or system.

Blogging means the process of writing or updating a "blog," which is an online, user-created journal short for "web log"."

BYOD means "Bring your own device." This is any personally owned equipment used on premises or to remotely access the college's network for the purpose of working. This includes desktops, laptops, smartphones, tablets or any other device that can readily access the college's networks and systems in addition to or instead of company-supplied devices.

Consultant is a type of contractor who provides expert advice or services in a particular field. Consultants operate independently and are typically engaged for strategic or advisory functions rather than operational tasks.

Contractor or Adjunct Faculty is an individual or company engaged temporarily under a contractual agreement to perform specific services or fulfill specialized roles— such as IT, teaching, or consulting. These individuals are hired for a defined job at a set rate of pay and are not considered permanent employees. As such, they do not become regular staff members and are not eligible for employee benefits.

Digital signature is a type of signature that guarantees that the contents of a message have not been altered in transit. It validates the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document).

Denial-of-Service (DOS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Electronic Signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

E-mail - Electronic mail means any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email Header Information is metadata accompanying an email that provides details about its origin, route, and content. It includes the sender, recipients, time of sending, and technical details, helping track the email's path, ensure delivery, verify authenticity, and manage security.

Employee Is an individual hired by Hebrew College on a full-time or part-time basis to perform duties under the direction and control of the College. Employees are typically eligible for benefits and are subject to the College's employment policies.

Encryption means a method for rendering information unusable to anyone without a "key" with which they are able to "translate" the information into a readable format. The process involves translating readable data into hidden data through the use of scrambling algorithms and a "key" which permits authorized users to unscramble the data into a usable format.

Extranet means a private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized Users within an organization.

FTP (File Transfer Protocol) – FTP is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.

Information Technology Resources includes any hardware, software, physical or digital data or any other areas that are provided by, supported by or overseen by the Director of Information Technology and the CIT team.

Instant Messaging means a text-based computer application, like teams or Facebook Messenger, which allows two or more internet-connected users to "chat" in real time.

Internet means a global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

Intranet means a private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only within an organization.

Metadata is information about other data. It describes details like the source, purpose, creation time, and structure of the data. For example, a photo's metadata might include the date it was taken and the camera settings. Metadata helps organize and understand data better.

Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

Peer-to-Peer (P2P) File Sharing means a distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Protected Health Information or PHI means information that is linked to, or could be linked to, a specific person by name, Social Security number (SSN), date of birth (DOB), geographic area or other individually identifiable information, and is related to that person's past, present, or future physical or mental health condition; the provision of health care to that person; or the payment for the provision of health care.

Personally Identifiable Information or Pll means information that can be used alone or in conjunction with any other personal information to identify a specific individual. Pll includes any information that can be used to search for or identify individuals or can be used to access their records. Social Security numbers, mailing or email address, and phone numbers have most commonly been considered PII, but technology has expanded the scope of PII considerably. It can include an IP address, login IDs, social media posts, or digital images.

Ransomware is a type of malware that hackers/criminals use to extort money. Ransomware locks your system files and data and restricts you from accessing the files until a ransom is paid.

Remote Desktop Access means remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Secure Email – Secure or encrypted email is a method of protecting sensitive email to protect it from being intercepted and/or manipulated. This can be accomplished through several technologies that include but are not limited to digital signatures, encryption or a secure gateway.

Secure Signature Software is a digital tool designed to create, manage, and authenticate electronic signatures with high levels of security. It ensures the authenticity and integrity of signed documents through features like encryption, identity verification, and audit trails. By using secure signature software, individuals and organizations can safely sign and share documents electronically, protecting against fraud and unauthorized use.

Services are technology-enabled functions provided to users, such as email, file storage, internet access, remote access, cloud applications (e.g., Microsoft 365), and help desk support. These services are governed by college policies and may be subject to monitoring and access controls.

Sniffing is an action whereby attackers monitor and/or record the routing exchanges between authorized routers to sniff for routing information. Attackers can also sniff data traffic information.

SPAM – Spam is "Unsolicited Bulk Email". Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content. A message is Spam only if it is both Unsolicited and Bulk.

> Unsolicited Email is normal email (examples: first contact enquiries, job enquiries, sales enquiries)

Bulk Email is normal email (examples: subscriber newsletters, customer communications, discussion lists)

Spoofing occurs when an illegitimate device or user assumes the identity of a legitimate one. This is most common in email when an email is delivered to an inbox and the “From:” address appears different than the actual sending email address.

Streaming Media means information, typically audio and/or video, which can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

Student Workers and Volunteers are typically engaged for short-term or part-time roles to support operational needs. These individuals may be hired directly or through third-party arrangements and are not entitled to long-term employment benefits. They are often granted access to institutional systems and resources under the same usage and security policies as regular users.

Systems are the integrated set of hardware, software, and network components used to support the College’s operations. This includes operating systems, databases, email platforms, learning management systems, and enterprise applications.

Temporary Worker/Student Work/Volunteer are individuals employed for a limited duration to meet short-term staffing needs. Temporary workers may be hired directly or through a staffing agency and are not entitled to long-term employment benefits.

Third-Party Affiliate Is any individual or entity not directly employed by Hebrew College but granted access to college systems or resources through a formal relationship (e.g., vendors, partners, or service providers). These individuals are bound by the same usage and security policies as internal users.

User means an individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

Vendor means any non-employee person or entity that exchanges goods or services (typically commercial goods and services) for money.

Volunteers offer their time and services to an institution without financial compensation. They willingly support activities, events, or projects such as organizing events, mentoring students, or helping in administrative tasks. Volunteers are not employees but play a vital role in the institution's operations and community engagement.

VPN stands for virtual private network which extends a private network across a public network and enables users to securely send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

4. POLICY

4.1. Policy Statement

This policy is designed to ensure that Hebrew College guidelines are clear concerning the use of computer assets and communication systems. Hebrew College will try to respect the individual privacy of its employees, but employee privacy does not extend to the employee's work-related conduct or to the use of Hebrew College applications/data systems and Hebrew College-issued equipment or supplies. Employees should be aware that the following guidelines may affect their privacy in the workplace.

4.2. Responsible Personnel

The Data Management Group is responsible for the periodic review, updating and administration of this policy. If you have any questions regarding this policy or if you have questions about use of Hebrew College's computer assets or communication systems that are not addressed in this policy, please contact the IT Department.

4.3. Authorities Delegated and Retained/Administrative Responsibility

The Chief Financial & Administrative Officer (CFAO) of the college delegates administration of the college's Acceptable Use of Information Technology Resources Policy to the Director of Information Technology.

4.4. General Use and Ownership

Hebrew College proprietary information stored on systems and devices, whether owned or leased by Hebrew College, the employee, or a third party, remains the sole property of Hebrew College. Employees must ensure through legal and technical means that Hebrew College's proprietary information is protected in accordance with Hebrew College's Confidentiality Policy.

Employees have a responsibility to report promptly the theft, loss, or unauthorized disclosure of Hebrew College's confidential and proprietary information.

Employees may access, use, or share Hebrew College confidential and proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties.

Employees must not store personal files such as music, video, photographs or games on Hebrew College resources.

4.5. Right to Access Information

Email, instant messaging, telecommunication systems, and data networks may have been installed by Hebrew College to facilitate business communications and information storage. By using an Electronic Signature to communicate with others, you acknowledge and agree that your Electronic Signature will have the same legal effect as your handwritten signature. Although an employee may have individual passwords and/or an Electronic Signature to access college resources, these resources belong to Hebrew College. The contents of e-mails, voice mail, or instant messaging may be accessed by Hebrew College's Center for Information technology (CIT), Human Resources (HR), or legal representation when required for business or lawful purposes. Individual managers may request delegated access to the mailboxes of their staff for legitimate business purposes.

All communications, including voice, text, and images, can be monitored and/or disclosed to law enforcement or other third parties without the prior consent of the sender or the receiver. Hebrew College will attempt to protect the confidentiality of employee information; however, employees should not assume that any message sent by email, voice mail, or instant messaging systems is confidential.

Employees should not assume electronic communications (especially cellular and digital telephones) are private, and should transmit Hebrew College confidential data, especially trade secrets, in other ways, such as secure email.

All information and communications sent or received through Hebrew College systems must be treated as company information and may not be used or shared with others for non-Hebrew College business either during or after employment with Hebrew College.

Providing an electronic signature on behalf of a colleague is prohibited unless that approval has been documented (e.g., with an email message) for one or multiple instances. Approval of a colleague to use an electronic signature must include an end-date.

Do not use Hebrew College's name, brand names, logos, taglines, slogans, or other trademarks without written permission from the Hebrew College Legal Advisors.

4.6. Personal Use of Hebrew College Telecommunications,

4.6.1. Email, Voice Mail, Instant Messaging or Internet Systems

Hebrew College provides these systems to assist employees in the performance of official Hebrew College business. Occasional personal use is permitted, but this usage should not disrupt normal business functions, systems, or processes. Use of email or the Internet should not disrupt the operation of Hebrew College's network or interfere with an employee's productivity. Employees should recognize that the Internet is a public domain and that they may therefore come in contact with information that a reasonable person would find offensive, sexually explicit, or inappropriate. Users of the Internet do so at their own risk. All handling of any sensitive information must conform with the rules of the Written Information Security Program (WISP)[1] including encrypting emails where necessary or accessing email or sensitive files on an open network like a public establishment or airport. Hebrew College is not responsible for any information that users view, read, or download from the Internet. Hebrew College reserves the right, in its sole and absolute discretion, to determine the appropriate level of personal use and to monitor this use by way of automated tools.

Personal or non-business-related data should not be stored on Hebrew College computer assets and communication systems.[2] For more information, please see the Hebrew College Network Protection and Information security Policy. (Sec. 3.5.2 as of 1/21/21)

4.6.2. Personal Data

The College makes every effort to maintain, backup and secure all data needed for business purposes. However, the College bears no responsibility to maintain, backup, or secure any personal data that employees or students may have on their computers' hard drives. Such personal files (including any digital music files) are the sole responsibility of the employee or student. Personal or non-business-related data should not be stored on Hebrew College computer assets and communication systems unless doing so has been 1) approved by the Data Steward responsible for digital data security and 2) instruction has been given on use of OneDrive for this purpose."

4.6.3. Personal Property

The College does not have the resources to support, or trouble-shoot problems employees or students may have with their personally owned computers also known as BYOD (Bring your own device).

There are many repair options outside the College that employees and students can use. Similarly, software that is provided for use on college computers is generally NOT available for use on employees' or students' personal home computers.[3]

---

[1] See: https://hebrewcollege.edu/wp-content/uploads/2020/12/Hebrew-College-Written-Information-Security-Program-WISP.pdf

[2] For more information on personal use of Hebrew College Telecommunication resources, please see the Hebrew College Network Protection and Information security Policy. (Sec. 3.5.2 as of 1/21/21)

[3] Further details of the Personal Property policy can be found in the Hebrew College Help Desk Support Policy in section 9.3

Hebrew College is not responsible for maintaining or repairing BYOD (Bring your own device). CIT personnel are prohibited from touching or instructing anyone to make changes or install software without consent from the Director of Information Technology (DIT).

BYODs must meet the minimum standards including password protection policies, up to date operating system (OS) and virus scan protection when connecting to Hebrew College digital and physical resources which include and is not limited to the on-premise network and cloud technology.

5. Internet Filtering

Every attempt to protect employee privacy will be maintained during day -to-day work practices. However, automated observation of Internet traffic flow has implemented technology that scans incoming and outgoing internet content for any content that is inappropriate or would put the institution at risk. This technology may flag any transaction, search or other content and alert CIT to review what has been flagged. It may be necessary, at the College's discretion, to delve into a person's internet history, downloads or content of a particular computer for security and legal reasons. The end-user who originates Internet traffic is responsible for Internet traffic that does not conform to this policy.

Hebrew College will use content filters, packet shapers, firewalls, spam filters, anti-virus and malware detection and other techniques to restrict access to inappropriate information on the Internet by students, faculty, staff and the community at large in all areas of the campus including classrooms, libraries and offices and on private and public wireless networks maintained by Hebrew College.

The College may also restrict access to sites on the Internet which results in excessive use of the College's information technology bandwidth.

Students, faculty, and staff may find that an Internet site is blocked intentionally, or a legitimate Internet site is unintentionally blocked. Requests to block or unblock an Internet site(s) must be submitted to the helpdesk with the URL that was accessed or blocked and a brief description of what the site represents. Each request will be forwarded to the Data management Team and one of the following representatives for review:

- Students – Director of Student Life
- Faculty – Chief Academic Officer
- Staff – Director of Human Resources

If the request is determined to be valid, the representative will inform the Center for Information Technology (CIT) via helpdesk system, and the site will be blocked or unblocked as appropriate. A notification will be sent to the originator of the request and the representative indicating the request has been honored. In the event the request is determined to be invalid, an explanation will be provided to the requestor by the representative.

6. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities, in the sole and absolute discretion of their supervisor(s) or the HR Department, as appropriate.

Under no circumstances is an employee of Hebrew College authorized to engage in any activity that is illegal under local, federal, or international law while using Hebrew College applications/data systems and Hebrew College-owned resources.

The list below is by no means exhaustive but attempts to provide a framework for activities that fall into the category of unacceptable use.

6.1. The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Hebrew College. This includes photocopying of copywritten text in any publications where copyright laws are enforced.
- Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular business duties. For the purpose of this section, "disruption" includes, but is not limited to, network sniffing, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior written authorization from CIT Director is obtained.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Forging of electronic signatures used in contracts and other agreements., You may not use any electronic signature in any form other than your own. To prevent such behavior, users should use secure signature software. Choose reputable electronic signature software that offers strong security features like encryption and two-factor authentication.
- Interfering with or denying service to any user other than the employee's host.
- Peer-to-Peer (P2P) networking is not allowed on the college network except in specific controlled tests of monitoring and blocking hardware and/or software.
- Streaming media consumes significant network resources and should be used judiciously. While reasonable use is permitted so long as it does not negatively impact on the computer network or hinder job performance.
- Using any program/script/command, or sending messages of any kind, with the intent of interfering with, or disable, a user's terminal session, by any means, locally or through the Internet/Intranet/Extranet.
- Sending, retrieving, or storing any communications in violation of the Hebrew College Harassment Policy. Please refer to the Hebrew College Employee Handbook for more information.
- Unauthorized use, or forging, of email header information.
- Signing up for illegal, unreliable, disreputable or suspect websites and services.
- Sending SPAM Or any unauthorized marketing content or solicitation emails.

- Soliciting for, or promoting of, commercial ventures, religious or personal causes, outside organizations, or other similar, non-job-related solicitations.
- Making fraudulent offers of products, items, or services originating from any Hebrew College account.
- Causing congestion on the network by such things as

  1) The propagation of "chain letters"; and/or

  2) "Broadcasting" inappropriate messages and/or attachments to lists of individuals; and/or

  3) The use of other bandwidth intensive applications such as unauthorized Internet downloads, gaming or video streaming.
- Intercepting, disrupting, or altering other electronic communication packages.
- Revealing your login password to others or allowing use of your login username and/or password by others. This includes, but is not limited to, family and other household members when work is being done at home.4
- Using someone else's identity, user ID, or password. The sharing of personal user IDs or passwords is strictly prohibited. Group\Shared mailboxes established to support business processes are exempt.
- Using the systems for any other purposes that are illegal, against Hebrew College's policies, or contrary to Hebrew College's best interests.
- The systems shall not be used to access, distribute, or publish Hebrew College's trade secrets or confidential or proprietary information without proper authorization, or in violation of Hebrew College's policies, or contrary to Hebrew College's best interests.
- Storing of any Hebrew College data outside an approved Hebrew College repository (e.g., Hebrew College file servers, etc.) is prohibited. Use of thumb drives should be limited to data generally available for public consumption. Storage of data and subscription services for storage of data such as Box.com, DropBox, Google Drive etc., are not to be used or contracted without express approval by the Data Management Group.
- For the official Hebrew College stance on passwords, please refer to the Hebrew College Password Policy available from the Director of Information technology for the latest copy. For your convenience a version of this policy is also available in Appendix C. 5

7. Blogging and social media social media [6][7]

Blogging or use of social media by employees using Hebrew College property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy as well as the Hebrew College Acceptable use policy. Limited and occasional use of Hebrew College systems to engage in blogging or access social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Hebrew College's policies, and does not interfere with

[4] For more information about the Password policy, see the Hebrew College Password Policy for greater details.
[5] See: Hebrew College Password Policy.docx
[6] See: Hebrew College Social Media Guidelines for Staff Faculty and Students_121922 (002).docx
[7] See: http://hebrewcollege.edu/wp-content/uploads/2023/06/Hebrew-College-Social-Media-Guidelines-for-Staff-Faculty-and-Students_121922-002.pdf

an employee's regular work duties. Blogging and use of social media from Hebrew College's systems is also subject to monitoring.

Hebrew College encourages all employees to communicate openly and transparently, for the benefit of Hebrew College, your colleagues, community-wide and yourself. With regard to participation in social media on behalf of Hebrew College, it is required to obtain management approval in advance and to focus your contributions on topics related to your position. Every Hebrew College employee has been given of the Hebrew College Employee handbook. Act according to the guidelines provided in this handbook.

These guidelines also apply when communicating on-line.

- Every employee is personally responsible for the content they publish on blogs, wikis or any other form of user-generated media internally and externally. Employees are prohibited from revealing any Hebrew College confidential or proprietary information, trade secrets, or any other material when engaged in blogging or using social media.
- Employees shall not make any discriminatory, defamatory, or harassing comments when blogging or using social media on Hebrew College's systems (e.g., ethnic slurs or sexist or discriminatory comments).
- Employees may also not attribute personal statements, opinions, or beliefs to Hebrew College when engaging in blogging or using social media. If an employee is expressing his or her beliefs and/or opinions in blogs or social media, the employee may not, expressly or implicitly, represent himself or herself as an employee or representative of Hebrew College. Employees assume any and all risk associated with this activity.
- Identify your name and, when relevant, role at Hebrew College, when you discuss Hebrew College or Hebrew College related matter externally and write in the first person. You must make it clear that you are speaking for yourself and not on behalf of Hebrew College. You can use a disclaimer such as the postings on this site are my own and don’t necessarily represent Hebrew College’s position, strategies or opinions.
- Respect copyright, fair use and financial disclosure laws.
- Don’t provide any confidential information or information that is meant to be private or confidential to Hebrew College.
- Don’t cite or refer to students, partners, colleagues or vendors without their approval.
- Respect your audience. Don’t engage in any conduct that would not be acceptable in Hebrew College’s workplaces.
- Try to add value. Provide worthwhile information and perspective.
- Hebrew College’s brand is best represented by its people and what you publish will reflect on Hebrew College’s brand, your colleagues and yourself.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Hebrew College's trademarks, logos, and any other Hebrew College intellectual property may also not be used in connection with any blogging or social media activity except where expressly permitted for marketing purposes.
- Don’t talk about our competitors.
- Stop publishing if your manager says so.

- This policy is not intended to restrict communications or actions protected or required by state or federal law.
- For more information, please see the Hebrew College Social Media Guidelines for Staff, Faculty, and Students available from the Director of Information Technology.

8. Hardware Usage

8.1. Purchase and Installation of Computing Hardware, Software, and Telecom Systems

All purchases of computing hardware, software, and telecommunication systems must be approved and coordinated by the IT Department to ensure compliance with institutional standards and ongoing support. In rare circumstances where senior management authorizes a purchase outside the usual process, collaboration with IT remains mandatory to guarantee proper integration, security, and supportability..

All computer equipment purchases must be coordinated by the Director of Information Technology before any purchases are made. Any purchases made prior to approval may need to be covered by their own department budget and may be subject to a different support level. CIT maintains an inventory of computer assets owned by the College. All computer equipment purchases must be made through the Director of Information Technology, as this allows Hebrew College to negotiate volume discounts and ensures that CIT is aware of every purchase.

All Hebrew College computer assets and communication systems will be maintained by authorized Hebrew College employees and/or agents who have been selected by Hebrew College to perform these functions. The installation or de-installation of computer equipment and/or software or shareware for use on the Hebrew College LAN/WAN must be performed by these individuals. THE INSTALLATION OR DE- INSTALLATION OF HARDWARE AND/OR SOFTWARE OR SHAREWARE BY NON-AUTHORIZED INDIVIDUALS IS STRICTLY PROHIBITED. For more information, please refer to the Hebrew College Computer Replacement and Purchase Policy available from the Director of Information technology.

8.2. Loaner and other Provided Equipment Use Policy

Introduction: We have observed a recent increase in issues related to our equipment, including breakage, misplacement, misconfiguration, and instances of missing items. Such occurrences are a cause for concern, especially considering our limited budgetary resources.

Policy Statement: In light of the costs and risks associated with the frequent movement of our Owls between rooms, it is imperative to establish a policy prohibiting their relocation under any circumstances. While there may have been isolated incidents where such movement was authorized out of necessity, it was never intended to become standard practice.

Guidelines:

1. **Restricted Use:** All utilization of the Owls must be confined to the rooms to which they are assigned. Despite their compact size and portability, it is essential to recognize the associated risks and refrain from moving them between locations. The facilities team has been instructed accordingly.
2. **Utilization in Designated Rooms:** Owls have been allocated to specific classrooms for use with associated TV or projector systems. Users are encouraged to utilize these devices within their designated spaces. Instructions for operation are provided in each room for ease of use.

3. **Exploring Alternatives:** In order to address limitations in video conferencing capabilities within certain rooms, efforts should be made to explore potential donors or funding sources willing to upgrade or enhance the technology infrastructure. This could potentially alleviate the need for relocating Owls and ensure consistent access to video conferencing capabilities across all spaces.

Conclusion: By adhering to these guidelines, we aim to mitigate the risks and costs associated with the movement and utilization of equipment, while ensuring efficient and effective communication and collaboration within our organization.

9. Security

9.1. Malware, Ransomware and Prevention of Viruses

By law and as stated in the Hebrew College WISP, all users must attend and pass a mandatory cybersecurity training program[8] to maintain access to Hebrew College resources and assets. Failure to do so will result in suspension of access to Hebrew College technical resources until training is complete.

Incoming files and/or software programs can pose a serious threat to IT systems. Viruses can destroy data not only on an employee's company-issued computer but also on Hebrew College's entire network. Program attachments also pose an additional threat by creating conflicts with the integration of the programs that run on an employee's personal computer. Although Hebrew College has a comprehensive virus protection system in place, Hebrew College places the following restrictions on its employees to prevent computer viruses from being transmitted through the systems:

- Avoid opening unsolicited messages and report any suspicious email to the IT Department. Delete all spam immediately. Do not reply to the message in any way, even if it states that you can request to be removed from its distribution list. If delivery persists, contact the IT Department, which will block any incoming email from that address.
- • The downloading or introduction of any unauthorized software, shareware, including executable files (.exe) or zipped (.zip) files from an unknown source, attached to emails and software acquired outside Hebrew College purchasing procedures or as part of doing usual Hebrew College business, into Hebrew College systems, without the authorization of Hebrew College's IT Department, is strictly prohibited.

Mandatory Annual Cybersecurity training is required by all employees.
Security is everyone's job. Virus infections can be avoided by being diligent. Exercise caution when downloading files through the Internet. If you suspect virus activity, it is your responsibility to report it to the IT Helpdesk and ensure it is remediated. Intentionally or negligently inflicting any computer virus infection through the downloading of executable files and/or software upon the Hebrew College LAN/WAN is grounds for immediate disciplinary action, up to and including termination of employment.

9.2. Information Security

9.2.1. PHI and PII protection

In general, confidential information, including Protected Health Information (PHI) and Personally Identifiable Information (PII) must not be: (I) shared or disclosed in any manner to individuals who are

[8] See: Hebrew College Security Awareness Training and Testing Policy.docx

not authorized Hebrew College employees or authorized employees of a Hebrew College customer; (ii) posted on the Internet or any publicly accessible systems; or (iii) transferred in an insecure manner. Specific policies and procedures for the protection and use of confidential information can be found in the Hebrew College WISP.

9.3. Confidentiality

Consistent with the Hebrew College Confidentiality guidelines present in the employee handbook[9], sensitive or vulnerable information should be encrypted or otherwise secured from unauthorized access.

In accordance with the Hebrew College Incident Response Plan[10], if a security incident or breach of any security policies is discovered or suspected, the user must:

Notify his or her direct supervisor or manager immediately to report the issue.

- Contact the IT Department, the Director of Information Technology, or any member of the Data Management Team to report the issue in detail and get a direct set of instructions.
- In the event of a lost or stolen laptop or external data drive, provide an inventory of sensitive data to the IT Department and the Incident Response team
- In the event of a lost or stolen phone, contact the IT Department so they can evaluate the risk and take appropriate steps to remediate the incident (e.g., remotely wipe the phone).

Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains Hebrew College or personal information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact Hebrew College's information security.
- Evidence that an employee has maliciously altered Student Information System (SIS) records, including changing individual records without cause, creating prank automated messaging, or altering employee/student permissions.
- Signs of Ransomware

Users must treat a suspected security incident as confidential information and report the incident only to their supervisors. Users must not, however, withhold information relating to a security incident or interfere with an investigation. Additional information on incident response can be found in the Hebrew College Incident Response Policy available from the Director of Information Technology.

[9] See page 9: Hebrew College Employee Handbook - September 2023.pdf
[10] Refer to the Hebrew College Incident Response Plan section 6.1 for any updates or changes to this section.

9.4. Multi Factor Authentication

9.4.1. Why Hebrew College has implemented Multi -Factor Authentication (MFA)

MFA stands for multi-factor authentication. It is a second line of computer system defense that makes sure whoever is using a username, and password is who they say they are. Password theft is the leading cause of network breaches. If someone has their password stolen, having another layer of authentication will help protect that account.

- It is a recommended standard for all cloud accounts. It is required by many banking institutions and anywhere that personal information or resources can be accessed. CJP is recommending it as well.
- Moving to the cloud has created better availability to our data but also created some security challenges. Before going to the cloud our first line of defense was governed by the physical access to the building, rooms and resources. Someone would need access to the building to break into someone's account.
- Secure against identity theft via stolen passwords. With access to someone's email account, a perpetrator could easily send and receive important emails with the stolen credentials
- Help protect us from unmanaged PCs and other devices. All HC pcs are managed by us. We can't guarantee that user-owned devices or public computers have the same type of security. MFA will add a second layer of protection.
- Compliance. Our insurance vendor has asked for a second type of authentication to safeguard our systems. The Business office is using their home IP address to access the remote desktop by only allowing those locations access to the server. ADP requires us to use MFA when we want to get our paycheck stubs.
- Using MFA reduces the chance of stolen login information being used to send spam, divert direct deposits, change tuition payments, or cancel registration, all to have funds sent to a hacker's account or gain access to restricted data.
- The FBI is strongly recommends the use of multi factor authentication. See: https://blog.knowbe4.com/heads-up-fbi-warns-about-attacks-that-bypass-your-multi-factor-authentication-mfa
- Cybercriminals are consistently coming up with new scams, tricks, and technology to get your data. Adding this type of layer makes it harder for them

The following methods are authorized for you in compliance with MFA

- Text or call - When you log in, O365 sends a text to your phone with a PIN that you must enter as a second level of identity authentication.
- Email - When you log in, O365 sends an email to a different account, most likely a personal account, with a PIN that changes every 30 seconds
- A Phone App - You can install the Microsoft authenticator app on your phone. When you try to log in, an alert will pop up on your phone asking if you want to grant access to the Hebrew College O365 cloud

- Biometrics - Facial recognition, thumbprint scanner, or a USB security device that is similar to a flash drive. authentication (MFI) also recognized as two factor authentication (2FA)

9.5. Hebrew College Automatic Email Forwarding Policy

To safeguard student Personally Identifiable Information (PII) and ensure compliance with federal and state data protection laws—including FERPA (Family Educational Rights and Privacy Act)—Hebrew College prohibits the automatic forwarding of college-issued email (@hebrewcollege.edu) to personal email accounts.

This policy applies to all Hebrew College faculty, staff, students, contractors, and volunteers who are issued a @hebrewcollege.edu email address.

Effective Nov 10, 2025, Hebrew College will implement a technical rule that blocks automatic forwarding of college emails to external domains such as Gmail.com, AOL.com, Yahoo.com, and others. This decision aligns with our commitment to maintaining the confidentiality, integrity, and availability of sensitive institutional data, particularly student PII.

Forwarding college emails to personal accounts:

- Circumvents institutional security controls, including multi-factor authentication (MFA), endpoint lockdown procedures, and real-time threat monitoring.
- Removes emails from protected environments, disabling automated scanning for sensitive content, virus detection, and patch management.
- Increases risk of unauthorized access, especially when forwarded to unmonitored or outdated personal devices.
- Violates FERPA and other data protection laws, potentially exposing the college to legal liabilities and financial penalties.

9.5.1. Legal and Regulatory Compliance

Hebrew College is obligated to comply with:

- FERPA, which mandates the protection of student education records and restricts unauthorized disclosures.
- Massachusetts Student Records Regulations (603 CMR 23.00), which define authorized access and disclosure protocols. [mass.gov]
- Other applicable federal and international data protection laws, including GDPR where relevant.

10. Copyright

Employees may not distribute over the systems any copyrighted materials belonging to any individual or entity other than Hebrew College. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify, or forward copyrighted materials, except with the permission of the holder of the copyright, or as a single copy to reference only. Stolen or bootleg copies of software are not allowed on any Hebrew College computing systems. All shareware programs must be registered in accordance with their license and use provisions. Employees shall not knowingly violate any software licenses, including without limitation, by making illegal copies of software. All software licenses, manuals, and documentation must be made available by the relevant department or branch for inspection in the event of a software inventory or audit. Failure

to observe copyright or license agreements may result in disciplinary action, up to and including termination of employment. See the EDUCOM Code for details on in Appendix A[11]

11.Violation

The use of Hebrew College-provided email, voicemail, telecommunications, and Internet systems in violation of this Acceptable Use Policy may lead to disciplinary action, which may include but is not limited to sanctions such as suspension, revocation of access privileges, or termination of employment. In instances of illegal activity, Hebrew College reserves the right to report such violations to appropriate legal authorities as necessary.

12.Acknowledgment of Receipt

By reviewing this document, you acknowledge your obligation to comply with the Hebrew College Acceptable Use of Information Technology Resources Policy. To confirm receipt and acceptance, you will be asked to sign an electronic acknowledgment (such as via DocuSign or a similar platform). Violations of this policy may result in the loss of computing privileges, probation, suspension, and/or up to and including termination of employment.

Historical Data of all Changes to Document

Revision History

Date	Name	Description of Change
7/27/18	Creation	Policy Created
9/3/20	Approved	Policy approved by the Data Management Group
11/12/20	Revisions and review	IT Director and HR Director met to review and update policy
1/12/21	Revision	Spell check and comments
7/2025 – 11/05/25	Revision Updates	Annual review of document and updates regarding several policies. Status changed from Added sections for Password Policy, incident response, MFA and email forwarding. Discussed @ DMG Meeting

[11] EDUCAUSE, who created the EDUCOM Code, has significant influence and authority as a leading voice for the higher education technology community. See Appendix A EDUCOM Code

Appendix A. EDUCOM Code

The EDUCOM Code was created in 1987; there are no plans for this code to be updated.

---

1. Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community

Source:

Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community issued by EDUCOM and ADAPSO

Software enables us to accomplish many different tasks with computers. Unfortunately, in order to get their work done quickly and conveniently, some people justify making and using unauthorized copies of software. They may not understand the implications of their actions or the restrictions of the U.S. copyright law.

Here are some relevant facts:

1. Unauthorized copying of software is illegal. Copyright law protects software authors and publishers, just as patent law protects inventors.
2. Unauthorized copying of software by individuals can harm the entire academic community. If unauthorized copying proliferates on a campus, the institution may incur legal liability. Also, the institution may find it more difficult to negotiate agreements that would make software more widely and less expensively available to members of the academic community.
3. Unauthorized copying of software can deprive developers of a fair return for their work, increase prices, reduce the level of future support and enhancement, and inhibit the development of new software products.

Respect for the intellectual work and property of others has traditionally been essential to the mission of colleges and universities. As members of the academic community, we value the free exchange of ideas. Just as we do not tolerate plagiarism, we do not condone the unauthorized copying of software, including programs, applications, databases and code.

Therefore, we offer the following statement of principle about intellectual property and the legal and ethical use of software. This "code"--intended for adaptation and use by individual colleges and universities--was developed by the EDUCOM Software Initiative.

2. Software and Intellectual Rights

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to the works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

3. Questions You May Have About Using Software

3.1. A. What do I need to know about software and the U.S. Copyright Act?

Unless it has been placed in the public domain, software is protected by copyright law. The owner of a copyright holds exclusive right to the reproduction and distribution of his or her work. Therefore, it is illegal to duplicate or distribute software or its documentation without the permission of the copyright owner. If you have purchased your copy, however, you may make a back-up for your own use in case the original is destroyed or fails to work.

3.2. B. Can I loan software I have purchased myself?

If your software came with a clearly visible license agreement, or if you signed a registration card, read the license carefully before you use the software. Some licenses may restrict use to a specific computer. Copyright law does not permit you to run your software on two or more computers simultaneously unless the license agreement specifically allows it. It may, however, be legal to loan your software to a friend temporarily as long as you do not keep a copy.

3.3. C. If software is not copy-protected, do I have the right to copy it?

Lack of copy-protection does not constitute permission to copy software in order to share or sell it. "Non-copy-protected" software enables you to protect your investment by making a back-up copy. In offering non-copy-protected software to you, the developer or publisher has demonstrated significant trust in your integrity.

3.4. D. May I copy software that is available through facilities on my campus, so that I can use it more conveniently in my own room?

Software acquired by colleges and universities is usually licensed. The licenses restrict how and where the software may be legally used by members of the community. This applies to software installed on hard disks in microcomputer clusters, software distributed on disks by a campus lending library, and software available on a campus mainframe or network. Some institutional licenses permit copying for certain purposes. Consult your campus authorities if you are unsure about the use of a particular software product.

3.5. E. Isn't it legally "fair use" to copy software if the purpose in sharing it is purely educational?

No. It is illegal for a faculty member or student to copy software for distribution among the members of a class, without permission of the author or publisher.

4. Alternatives to Explore

Software can be expensive. You may think that you cannot afford to purchase certain programs that you need. But there are legal alternatives to unauthorized copying.

5. Site Licensed and Bulk-Purchased Software

Your institution may have negotiated agreements that make software available either to use or to purchase at special prices. Consult your campus computing office for information. Software available through institutional site licenses or bulk purchases is subject to copyright and license restrictions, and you may not make or distribute copies without authorization.

6. Shareware

Shareware, or "user-supported" software, is copyrighted software that the developer encourages you to copy and distribute to others. This permission is explicitly stated in the documentation or displayed on the computer screen. The developer of shareware generally asks for a small donation or registration fee if you like the software and plan to use it. By registering, you may receive further documentation, updates and enhancements. You are also supporting future software development.

7. Public Domain Software

Sometimes authors dedicate their software to the public domain, which means that the software is not subject to any copyright restrictions. It can be copied and shared freely.

Software without copyright notice is often, but not necessarily, in the public domain. Before you copy or distribute software that is not explicitly in the public domain, check with your campus computing office.

8. A Final Note

Restrictions on the use of software are far from uniform. You should check carefully each piece of software and the accompanying documentation yourself. In general, you do not have the right to:

1. Receive and use unauthorized copies of software, or
2. Make unauthorized copies of software for others.

If you have questions not answered by this brochure about the proper use and distribution of a software product, seek help from your computing office, from the software developer, or publisher.

Appendix B. Ransomware Signs and Encrypted File Extensions List

Some signs that may indicate you have become a victim to Ransomware may include:

Inaccessible Files:

Users may find that they are unable to open files they previously had access to. Attempts to open files may result in error messages indicating that the files are corrupted or damaged.

Renamed File Extensions:

Ransomware often alters file extensions to ones that are unfamiliar or specifically designed for the ransomware (e.g., changing .docx to. locked or .crypto). Users might notice unfamiliar file extensions on their documents.

Ransom Note:

A prominent sign of ransomware infection is the presence of a ransom note that appears on the screen or in affected folders. This note typically demands payment in exchange for restoring access to files.

Unusual System Behavior:

Systems may exhibit strange behavior, such as slowed performance, unexpected pop-ups, or applications crashing or behaving erratically.

High Disk Activity:

Users may notice high disk usage or CPU activity that appears to be the result of unauthorized encryption processes running in the background.

Missing Files:

Certain files may be missing altogether, either deleted or encrypted in such a way that they are no longer visible.

Presence of New or Unknown Processes:

Users may observe unfamiliar processes running in the task manager that might indicate the presence of malicious software.

Backup Files Compromised:

Ransomware may also target backup files or systems, making it difficult to recover data even if backups were in place.

Alerts from Security Software:

Security solutions may detect abnormal activities or flag files as potentially malicious, serving as an early warning of an infection.

The following is a list of known file extensions used by hackers to lock you out of your data:

Ref: https://techviral.net/ransomware-encrypted-file-extensions/ 9-19-20

WARNING: Some of the names of these definitions may be offensive to some and do not follow Acceptable Use Standards but are necessary for documentation purposes.

micro	TeslaCrypt 3.0 ransomware encrypted data
zepto	Locky ransomware affected data
cerber	Cerber ransomware affected data
locky	Locky ransomware affected data
cerber3	Cerber 3 ransomware affected data
cryp1	CryptXXX ransomware affected data
mole	CryptoMix (variant) ransomware affected data
onion	Dharma ransomware affected data
axx	AxCrypt encrypted data
osiris	Locky (variant) ransomware affected data
crypz	CryptXXX ransomware affected data
crypt	Scatter ransomware affected data
locked	Various ransomware affected data
odin	Locky ransomware affected file
ccc	TeslaCrypt or Cryptowall encrypted data
cerber2	Cerber 2 ransomware affected file
sage	Sage ransomware affected data
globe	Globe ransomware affected file
exx	Alpha Crypt encrypted file
good	Scatter ransomware affected file
wallet	Globe 3 (variant) ransomware affected file
1txt	Enigma ransomware affected file
decrypt2017	Globe 3 ransomware affected file
encrypt	Alpha ransomware affected file
ezz	Alpha Crypt virus encrypted data
zzzzz	Locky ransomware affected file
MERRY	Merry X-Mas ransomware affected file
enciphered	Malware (ransomware) encoded file
r5a	7ev3n ransomware affected file
aesir	Locky ransomware affected file
ecc	Cryptolocker or TeslaCrypt virus encrypted file
enigma	Coverton ransomware affected file
cryptowall	Encrypted file by Cryptowall ransomware
encrypted	Various ransomware affected file
loli	LOLI RanSomeWare ransomware affected file
breaking_bad	Files1147@gmail(.)com ransomware affected file
coded	Anubis ransomware affected file
ha3	El-Polocker affected file
damage	Damage ransomware affected file
wcry	WannaCry ransomware affected file
lol!	GPCode ransomware affected file
cryptolocker	CryptoLocker encrypted file
dharma	CrySiS ransomware affected file
MRCR1	Merry X-Mas ransomware affected file
sexy	PayDay ransomware affected files
crjoker	CryptoJoker ransomware affected file
fantom	Fantom ransomware affected file
keybtc@inbox_com	KeyBTC ransomware affected file
rrk	Radamant v2 ransomware affected file
legion	Legion ransomware affected file
kratos	KratosCrypt ransomware affected file
LeChiffre	LeChiffre ransomware affected file
kraken	Rakhni ransomware affected file
zcrypt	ZCRYPT ransomware affected file
maya	HiddenTear (variant) ransomware affected file
enc	TorrentLocker ransomware affected file
file0locked	Evil ransomware affected file
crinf	DecryptorMax or CryptInfinite ransomware affected file
serp	Serpent (variant) ransomware affected file
potato	Potato ransomware affected file
ytbl	Troldesh (variant) ransomware affected file
surprise	Surprise ransomware affected file
angelamerkel	Angela Merkel ransomware affected file
windows10	Shade ransomware affected file
lesli	CryptoMix ransomware affected file
serpent	Serpent ransomware affected file
PEGS1	Merry X-Mas ransomware affected file
dale	Chip ransomware affected file
pdcr	PadCrypt Ransomware script
zzz	TeslaCrypt ransomware encrypted file
xyz	TeslaCrypt ransomware encrypted file
1cbu1	Princess Locker ransomware affected file
venusf	Venus Locker ransomware affected file
coverton	Coverton ransomware affected file
thor	Locky ransomware affected file
rnsmwr	Gremit ransomware affected file

evillock	Evil-JS (variant) ransomware affected file
R16m01d05	Ransomware affected data
wflx	WildFire ransomware affected file
nuclear55	Nuke ransomware affected file
darkness	Rakhni ransomware affected file
encr	FileLocker ransomware affected file
rekt	HiddenTear (variant) ransomware affected file
kernel_time	KeRanger OS X ransomware
zyklon	ZYKLON ransomware affected file
Dexter	Troldesh (variant) ransomware affected file
locklock	LockLock ransomware affected file
cry	CryLocker ransomware affected file
VforVendetta	Samsam (variant) ransomware affected file
btc	Jigsaw Ransomware affected file
raid10	Globe [variant] ransomware affected file
dCrypt	DummyLocker ransomware affected file
zorro	Zorro ransomware affected file
AngleWare	HiddenTear/MafiaWare (variant) ransomware affected file
EnCiPhErEd	Xorist Ransomware affected file
purge	Globe ransomware affected file
realfs0ciety@sigaint.org.fs0ciety	Fsociety ransomware affected file
shit	Locky ransomware affected file
atlas	Atlas ransomware affected file
exotic	Exotic ransomware affected file
crypted	Nemucod ransomware affected file
padcrypt	PadCrypt ransomware affected file
xxx	TeslaCrypt 3.0 ransomware encrypted file
hush	Jigsaw ransomware affected file
bin	Alpha/Alfa ransomware affected file
vbransom	VBRansom 7 ransomware affected file
RMCM1	Merry X-Mas ransomware affected file
cryeye	DoubleLocker ransomware affected data
unavailable	Al-Namrood ransomware affected file
braincrypt	Braincrypt ransomware affected file
fucked	Manifestus ransomware affected file
crypte	Jigsaw (variant) ransomware affected file
_AiraCropEncrypted	AiraCrop Ransomware affecte file
stn	Satan ransomware affected file
paym	Jigsaw Ransomware affected file
spora	Spora ransomware affected file
dll	FSociety ransomware affected file
RARE1	Merry X-Mas ransomware affected file
alcatraz	Alcatraz Locker ransomware affected file
pzdc	Scatter ransomware affected file
aaa	TeslaCrypt ransomware encrypted file
encrypted	Donald Trump ransomware affected file
ttt	TeslaCrypt 3.0 ransomware encrypted file
odcodc	ODCODC ransomware affected file
vvv	TeslaCrypt 3.0 ransomware encrypted file
ruby	Ruby ransomware affected file
pays	Jigsaw Ransomware affected file
comrade	Comrade ransomware affected file
enc	Cryptorium ransomware affected file
abc	TeslaCrypt ransomware encrypted file
xxx	help_dcfile ransomware affected file
antihacker2017	Xorist (variant) Ransomware affected file
herbst	Herbst ransomware affacted file
szf	SZFLocker ransomware affected file
rekt	RektLocker ransomware affected file
bript	BadEncriptor ransomware affected file
crptrgr	CryptoRoger ransomware affected file
kkk	Jigsaw Ransomware affected file
rdm	Radamant ransomware affected file
BarRax	BarRax (HiddenTear variant) ransomware affected file
vindows	Vindows Locker ransomware affected file
helpmeencedfiles	Samas/SamSam ransomware affected file
hnumkhotep	Globe 3 ransomware affected file
CCCRRRPPP	Unlock92 ransomware affected file
kyra	Globe ransomware affected file

fun	Jigsaw Ransomware affected file
rip	KillLocker ransomware affected file
73i87A	Xorist Ransomware affected file
bitstak	Bitstak ransomware affected file
kernel_co mplete	KeRanger OS X ransomware file
payrms	Jigsaw Ransomware affected file
a5zfn	Alma Locker ransomware affected file
perl	Bart ransomware affected file
noproblem wedecfiles	Samas/SamSam ransomware affected file
lcked	Jigsaw (variant) ransomware affected file
p5tkjw	Xorist Ransomware affected file
paymst	Jigsaw Ransomware affected file
magic	Magic ransomware affected file
payms	Jigsaw Ransomware affected file
d4nk	PyL33T ransomware affected file
SecureCryp ted	Apocalypse ransomware affected file
paymts	Jigsaw Ransomware affected file
kostya	Kostya ransomware affected file
lovewindo ws	Globe (variant) ransomware affected file
madebyad am	Roga ransomware affected file
powerfulld ecrypt	Samas/SamSam ransomware affected file
gefickt	Jigsaw (variant) ransomware affected file
kernel_pid	KeRanger OS X ransomware file
ifuckedyou	SerbRansom ransomware affected file
grt	Karmen HiddenTear (variant) ransomware affected file
conficker	Conficker ransomware affected file
edgel	EdgeLocker ransomware affected file
PoAr2w	Xorist Ransomware affected file
oops	Marlboro ransomware affected file
adk	Angry Duck ransomware affected file
encrypted	KeRanger OS X ransomware affected file
Whereisyo urfiles	Samas/SamSam ransomware affected file
czvxce	Coverton ransomware affected file
theworldis yours	Samas/SamSam ransomware affected file
info	PizzaCrypts Ransomware affected file
razy	Razy ransomware affected file
rmd	Zeta ransomware affected file
fun	Jigsaw (variant) ransomware affected file
kimcilware	KimcilWare ransomware affected file
paymrss	Jigsaw Ransomware affected file
dxxd	DXXD ransomware affected file
pec	PEC 2017 ransomware affected file
rokku	Rokku ransomware affected file
lock93	Lock93 ransomware affected file
vxlock	vxLock ransomware affected file
pubg	PUBG ransomware affected data
crab	GandCrab ransomware affected data

List last update 3-4-21

Appendix C. Hebrew College Password Policy

Password Policy

Remote and local access to applications and systems is granted by authentication and authorization systems managed by the Center for Information Technology (CIT). In most cases, access is allowed via username and password.

Frequently, sensitive information is transmitted and stored in email, which can make it vulnerable to exposure on email servers, local computers (both at work and home), and during transmission. Users should avoid transmitting or storing sensitive information in email unless absolutely necessary, and only after ensuring the data is adequately encrypted using Outlook encryption.

Password Protection Policy

Passwords are a crucial component of our computer security program. A weak or compromised password can result in unauthorized access to critical Hebrew College resources. All Hebrew College staff, contractors, and vendors with system access must follow the guidelines below to select and secure their passwords.

Choosing Passwords

Users (defined as Hebrew College employees who are not part of the IT team) must select strong, difficult-to-guess passwords. Fixed passwords must be at least 8 characters long, and this minimum must be enforced by Active Directory Group Policy. Passwords must include alphabetic and numeric characters. Strong passwords should follow these guidelines:

Weak passwords:

- Common words, such as family or pet names, co-workers, fantasy characters, or birthdays
- Simple patterns, such as "123456," "qwerty," or "password"

Strong passwords:

- Contain both uppercase and lowercase letters (e.g., A-Z, a-z)
- Include digits and special characters (e.g., 0-9, !@$%^&()_+|~-=\`{}[]:";'<>?,./)
- Are not common words in any language
- Are not based on personal information

Changing Passwords

IT Support Professionals:

- All system-level passwords must be changed every 90 days.
- Administrative-level passwords for production environments are managed through Active Directory.
- System-level users must have unique passwords for accounts with elevated privileges.
- Passwords should not be reused or recycled, and fixed passwords must change every 90 days.
- Users (Non-IT Staff):
- Passwords must be changed every 90 days, and users must change their password upon first login.
- If a user suspects their password has been compromised, it must be changed immediately.
- CIT will not reset passwords without identity verification through valid government or Hebrew College ID.
- New hires receive temporary passwords, which they must change upon first logon.

Protecting Passwords

Users must take the following precautions to safeguard their usernames and passwords:

- Never share usernames or passwords with anyone, including colleagues, managers, or IT staff.
- Select strong passwords, incorporating letters, numbers, and special characters.
- Avoid entering passwords on compromised or public computers.
- Do not save passwords in browsers or unencrypted files.
- Default vendor passwords must be changed before use in Hebrew College systems.
- Do not store passwords online without encryption (e.g., text files, apps without encryption).
- Do not use the same password for Hebrew College accounts and personal accounts.
- Never reveal passwords over the phone, email, or in public conversations.
- If an account or password is suspected of being compromised, report it to the HelpDesk immediately and change the password.
- Lost or Stolen Passwords:
- If a password is lost or suspected to be stolen, it must be reported immediately to the HelpDesk. Failure to report or protect passwords may result in suspension of user access until a supervisor's approval is obtained. CIT may perform random desk checks for written-down passwords or unsecured workstations.

Azure Multi-Factor Authentication (MFA)

Hebrew College requires **Azure Multi-Factor Authentication (MFA)** as an additional layer of security for all system access. MFA is mandatory for all users and significantly enhances account security by requiring a second form of authentication in addition to the user's password.

What is MFA?

MFA, or Multi-Factor Authentication, is a security measure that requires users to provide two or more verification methods to gain access to a system. It combines something the user knows (password) with something the user has (a mobile device or authentication app) or something the user is (biometric data like a fingerprint or facial recognition).

At Hebrew College, we use Azure MFA, which typically involves:

- A password (the first factor)
- A secondary authentication method, such as:
- A text message with a code sent to your mobile phone
- A phone call to verify your identity
- An authentication app (such as the Microsoft Authenticator app) that generates a time-sensitive verification code

How to Use MFA:

- **Initial Setup**: Users will receive instructions to enroll in MFA during their account setup process. This will involve linking your mobile phone or authenticator app to your Hebrew College account.
- **Login Process**: After entering your password, a secondary prompt will ask for your authentication code (via text message or app). You must complete this second step to successfully log in.
- **MFA for Remote Access**: MFA is required for accessing Hebrew College systems remotely. Users will not be able to log in without completing this additional verification step.

- **Maintaining Security**: Users should ensure that their MFA method (such as mobile phone number) is kept up to date with CIT. If you change devices or phone numbers, contact CIT to update your MFA settings.

Importance of MFA:

MFA reduces the risk of unauthorized access to systems, even if a password is stolen or compromised. It ensures that only the authorized user can complete the login process, adding an essential layer of security to Hebrew College's resources.

Failure to comply with MFA requirements will result in restricted access to Hebrew College systems until MFA is properly configured.

Password Sharing Policy

Passwords are personal and should never be shared with anyone. This includes supervisors, co-workers, IT staff, and family members. Sharing passwords compromises the security of Hebrew College's systems and puts sensitive information at risk. **Under no circumstances should any user disclose their password to anyone**.

If a situation arises where access is required by another individual (such as IT staff), proper authorization and procedures must be followed, such as password resets or temporary access through official channels. Sharing passwords violates security protocols and may result in disciplinary action, including **account suspension.**

HelpDesk Support Policy for Passwords

In situations where CIT personnel must work on a user's computer without their presence, the following safeguards apply:

- Reschedule work for when the user is available to protect the password.
- If rescheduling is not possible, notify the user that their password will be temporarily changed to gain access, and set the password to "User must change password at next logon" after completion.
- In rare cases where neither option is feasible, users may share their password with CIT personnel, with approval from the Director of IT and the user's supervisor.

Keep in mind the following:

- Passwords must not be written down or stored where others can access them.
- Do not store passwords in unencrypted files or share them via email or phone.
- If a password is suspected of being compromised, notify the HelpDesk immediately and change the password.

Appendix D. Executive Summary: Hebrew College Acceptable Use of Information Technology Resources Policy

Purpose & Scope

This policy establishes clear standards for the responsible use of Hebrew College's information technology resources—including hardware, software, data, and communication systems. It applies to all employees, contractors, consultants, volunteers, student workers, and third-party affiliates who access college-owned or managed assets.

Key Principles

- IT resources are provided to support the educational mission and business activities of Hebrew College.
- Use of these resources is a privilege, not a right, and is subject to monitoring and review.
- Compliance with this policy is required for continued employment or engagement.

Major Policy Areas

General Use & Ownership

- All data and communications on college systems are Hebrew College property.
- Employees must protect proprietary information and report theft, loss, or unauthorized disclosure.
- Personal files should not be stored on college resources unless specifically approved and managed via OneDrive.

Privacy & Access

- Work-related conduct and system use may be monitored.
- Email, instant messaging, and other communications may be accessed for business or legal reasons.
- Delegated access to mailboxes is permitted for legitimate business purposes.

Unacceptable Use

Strictly prohibited activities include:

- Illegal activities under local, federal, or international law.
- Copyright violations, including unauthorized software or photocopying of protected materials.
- Introduction of malicious programs (viruses, ransomware, etc.).
- Security breaches, unauthorized access, or circumvention of authentication.
- Forging or misusing electronic signatures.
- Peer-to-peer networking and excessive streaming media use.
- Storing college data outside approved repositories (e.g., unauthorized use of Dropbox, Google Drive).
- Sharing passwords or using another person's credentials.

Security & Data Protection

Mandatory annual cybersecurity training for all users.

- Multi-Factor Authentication (MFA) is required for system access.
- PHI (Protected Health Information) and PII (Personally Identifiable Information) must be protected and not shared or transferred insecurely.
- Incident response procedures require immediate reporting of suspected breaches or security incidents.

Hardware & Software Management

- All purchases of computing hardware, software, and telecommunication systems must be approved and coordinated by the IT Department.
- In rare cases where senior management authorizes a purchase outside the usual process, collaboration with IT remains mandatory to guarantee proper integration, security, and supportability.
- Unauthorized installation or removal of equipment/software is prohibited.
- Loaner equipment (e.g., Owls for video conferencing) must remain in assigned rooms;

movement is not allowed.

Social Media & Blogging

- Limited personal use of college systems for blogging and social media is permitted if professional and does not interfere with work.
- Employees must not disclose confidential information or represent personal opinions as those of Hebrew College.
- Use of college trademarks, logos, or branding in social media requires written permission.

Copyright & Intellectual Property

- Employees must respect copyright and intellectual property rights.
- Unauthorized copying, distribution, or use of software and materials is prohibited.
- EDUCOM Code and guidelines for ethical software use are included in the appendix.

Enforcement & Violations

- Violations may result in disciplinary action, including suspension, revocation of access, or termination.
- Illegal activities may be reported to legal authorities.

Recent Updates (2025)

- Expanded definitions for employee types, volunteers, and third-party affiliates.
- Clarified rules for personal data storage and use of OneDrive.
- Enhanced MFA requirements and email forwarding restrictions to protect student PII.
- Updated procedures for incident response and ransomware detection.
- Revision history and change log included for transparency.

Practical Implications

- All users must follow password protection and MFA protocols.
- Personal use of IT resources is limited and monitored.
- Storing college data on unauthorized platforms is prohibited.
- Report any security incidents or suspicious activity immediately.
- Consult IT for hardware/software purchases and support.

Reference Documents

- Written Information Security Program (WISP)
- Employee Handbook
- Social Media Guidelines
- Password Policy
- Incident Response Plan
- EDUCOM Code of Software Ethics