Hebrew College Remote Work Policy

Responsible office	HR – Human Resources
Responsible party	DMG – Data Management Group
Last Save Date	6/8/2022
Status	Approved
Last revision #	4th
Approved by	Data Management Group
Approval date	6/8/2022
Effective date	6/8/2022
Last review	6/8/2022

Contents

1 Policy Statement

During Academic Years 2020-2022, most or all employees were required to work remotely for some period of time. Beginning in the winter of Academic Year 2022-2023, Hebrew College will operate from a new facility with newly created shared office space and required flex-time arrangements. Given these realities, the following policies and guidelines have been created to address remote work issues for all employees across the College. Remote access by faculty and staff is a method of accessing files and systems that is becoming more common today. In practice, the benefits of securing remote access are considerable – business can be conducted remotely with confidence and sensitive college information remains confidential. This document sets out the policy for remote access and includes a set of common controls, which can be applied to reduce the risks associated with a remote access service.

Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

2 Overview & Purpose

Any regular full-time or part-time employee who does not have a private, dedicated workspace at Hebrew College must be prepared to work remotely some of the time. All employees working remotely must have access to a computer and internet and must have access to Microsoft Office 365 in order to use Hebrew College documents, files and email.

It is the responsibility of Hebrew College's employees, contractors, and vendors with remote access privileges to keep Hebrew College's owned data and assets protected.

The purpose of this policy is to define the rules and requirements for connecting to our organization's network from any remote setting.

The goal of these requirements is to reduce the exposure of potentially sensitive Hebrew College data to any external malicious threat actors.

3 Scope

This policy applies to all employees, contractors, vendors and agents with a college-owned or personally owned computer or workstation used to connect to the network. This policy applies to remote access connections used to do work on behalf of, including reading or sending email and viewing secure web resources. This policy covers any and all technical implementations of remote access used to connect to networks.

4 Objectives

The objectives of the policy on remote access by staff are:

- To provide secure and reliable remote access to the College's information systems.
- To preserve the integrity, availability and confidentiality of the Hebrew College's information and information systems.
- To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.
- To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the Hebrew College is adequately protected under computer misuse legislation.

5 Risks

The Hebrew College recognizes that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

- unavailability of network, systems or target information
- degraded performance of remote connections
- loss or corruption of sensitive data
- breach of confidentiality
- loss of or damage to equipment
- breach of legislation or non-compliance with regulatory or ethical standards.

6 Responsibilities

- The Data Management Group is ultimately responsible for ensuring that remote access by staff is managed securely.
- The Director of Information Technology is responsible for providing clear authorization for all remote access users and the level of access provided.
- All remote access users are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources, notify the Hebrew College Director of Information Technology immediately of any security incidents and breaches.
- Upon termination from Hebrew College, all employees must return all relevant equipment to HR.

7 Expectations

7.1 College Policies

Employees must agree to comply with all Hebrew College rules, policies and practices while working remotely, including policies relating to information security and data protection (see related policies below under "Security.")

7.2 Hours Worked

The total number of hours that employees working remotely are expected to work does not change, regardless of work location. Hebrew College also expects the same level of productivity from employees working remotely that is expected from employees at the Hebrew College campus.

8 Internet Connectivity

As a prerequisite to working from home, the location the remote work is being done must have a stable, non-public internet connection with sufficient bandwidth to participate in video meetings and other regular activities. They must have audio and video capabilities. Employees are encouraged to speak with the helpdesk personnel before beginning remote work to assess the employee's equipment, such as their internet connection, pros and cons of wi-fi versus ethernet connections, router, age of personal computer, etc.

8.1 Loss of internet

An employee must speak with their supervisor to establish a protocol in the event of an internet outage in a remote location. If a solution is decided to find an alternate location other than on the Hebrew College Campus, be sure the new location adheres to the other guidelines expressed in this policy.

9 Security

Consistent with the organization's expectations of information security for employees working at the office, Remote work employees will be expected to ensure the protection of proprietary institutional and customer information accessible from their home office. Steps include the use of locked file cabinets and desks, regular password maintenance, and any other measures appropriate for the job and the environment.

Employees must safeguard Hebrew College information used or accessed while working remotely, in accordance with the College's "INFORMATION-SHARING DATA SECURITY GUIDELINES", "Acceptable Use of Information Technology Resources" policy and the employee handbook.

Employees working remotely must agree to follow College-approved security procedures in order to ensure confidentiality and security of data.

Employees working remotely must be cognizant of their physical and cyber space, to ensure that other persons (e.g., family members, workers in the home) do not have access to Hebrew College files, passwords, records, or equipment.

Employees who work remotely and have confidential files on paper must ensure that they have a secure, lockable space in their remote workspace in which to store these documents.

Multi Factor Authentication will be enforced for all non-compliant or BYOD devices

9.1 Reporting Security Incidents & Weaknesses

All security weaknesses and incidents must be reported to the Director of Information Technology through the IT Helpdesk at 617-559-8680.

10 Equipment

Employees who are required by the College to work remotely will be provided with certain equipment or expenses as agreed upon with the department manager. These include but are not limited to a Hebrew College-owned laptop computer, and any software applications which are necessary for the employee's work. On a case-by-case basis, Hebrew College will determine, with information supplied by the employee and the supervisor, the appropriate equipment needs (including hardware, software, and peripherals) for each Remote work arrangement. The human resources and information system departments will serve as resources in this matter. Equipment supplied by the organization will be maintained by the organization. Equipment supplied by the employee, if deemed appropriate by the organization, will be maintained by the employee. Hebrew College accepts no responsibility for damage or repairs to employee-owned equipment. Hebrew College reserves the right to make determinations as to appropriate equipment, subject to change at any time. Equipment supplied by the organization is to be used for business purposes only. The remote worker must keep track of all Hebrew College property received and agree to take appropriate action to protect the items from damage or theft. Upon termination of employment, all company property will be returned to the company, unless other arrangements have been made.

Employees may choose to use their own personal computers with the caveat that they agree to install software which is necessary to do their work (e.g., Microsoft Office 365 & VOIP Phone software), and that they understand the limitations on technical support that they will be able to access. Hebrew College reserves the right to examine an employee's personal computer's security settings and request upgrades at the employee's expense if the Director of Information Technology deems that the current security settings put Hebrew College data at risk.

The employee will establish an appropriate work environment within their home or other non-workplace location for work purposes. Hebrew College will not be responsible for costs associated with the setup of the employee's home office, such as remodeling, furniture, or lighting, nor for repairs or modifications to the home office space.

All equipment which Hebrew College provides to an employee, whether used on campus or in connection with remote work, remains the property of the College and must be returned upon separation from employment or at any other time upon notice from the College.

11 Safety

The College may use departmental budget dollars for remote work costs if there is a significant business need and funding permits for: Access to a phone, a Laptop PC and peripherals based on need and job function. Peripherals may or may not contain items like printers, scanners, monitors, wireless keyboard, mouse or another ergonomic equivalent.

Hebrew College is not responsible for the operating costs, maintenance, property or liability insurance, or other expenses for an employee's home or other remote work location.

12 Technical Support

Employees who are using their own personal computers will have access to Hebrew College IT for support of Office 365, other approved software, onsite internet access, approved vendor products such as Campus Café or Schoology and any other approved technology resources. Support will be limited to break fix of the product or service. If it is deemed the equipment is the point of failure for a particular issue, IT staff can guide employees to outside vendors for external support at the user's expense. Technology is constantly evolving; it is hard to predict what support scenarios the department will face in the future but they will be dealt with on a case by case basis and under the guidelines of the IT support policies. Any changes or updates to what is covered and what is not covered is the sole discretion of the Director of Information Technology.

12.1 Support Expectations

Remote workers are responsible for maintaining a consistent internet connection. The CIT team will do everything possible to identify possible issues with HC owned devices. If it is determined that the device is working correctly and that the issue is with the person's Wi-Fi signal or with their ISP, CIT personnel is unable to make or assist in making changes to any home networking equipment. This included cable modems, routers, Access Points and switches. It is the responsibility of the remote worker to contact their ISP and to maintain and troubleshoot their Internet connection.

Hardware and Software

Employees who are using Hebrew College equipment will have access to Hebrew College IT to troubleshoot both hardware and software issues.

Personal devices

Personally owned computers, macs, laptops and tablets, sometimes called BYODs (Bring Your Own Devices) can be used to access SharePoint and our cloud infrastructure. There is limited support for these devices and employees are encouraged to use an outside vendor for issues with personal equipment.

13 Validity of this Policy

This policy should be reviewed annually under the authority of the Data Management Group and the Director of Information Technology. Associated information security standards should be subject to an on-going development and review program.

14 Effective date

This Remote Work Policy was implemented June 2022.

The College will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.

15 Historical Data of all Changes to Document

Revision History

Date	Name	Description of Change
10/27/21	Creation	Policy Document drafted
4/5/22	Updates	Wording and policy updates from HR
6/8/22	Senior Management Sign off	Waiting for approval
		Waiting to be approved by the Data Management Group