DePaul University

Telecommuting

Category: Human Resources
Responsible Department: Benefits
Responsible Officer: Vice President, Human Resources
Effective Date: 8/30/2017

Policy Summary

The purpose of this policy is to specify the criteria for a telecommuting arrangement.

Scope

This policy affects the following groups of the University:

- Full-Time Staff

This policy affects all full-time staff members. Telecommuting is intended for full-time university staff employees, defined as employees who are scheduled to work at least 1,820 hours per calendar year and work in a position classified as full-time. Employees who have been on a "Performance Improvement Plan" or have received final written counseling may not request a telecommuting arrangement until 12 months have elapsed since the plan's end or the date of final written counseling, whichever is later. Employees on a leave of absence are not eligible for a telecommuting arrangement.

Policy

DePaul University recognizes that flexibility is desired in today's workplace to respond to the work-life balance needs of a diverse workforce. Telecommuting allows employees to perform a portion of their job responsibilities at an alternative work site while maintaining a full-time employment schedule. The employee's duties, obligations, responsibilities and conditions of employment with the University remain unchanged when the arrangement involves only a change in work location.

The decision to permit an employee to telecommute is at the discretion of the employee's manager, the nature of the employee's position and the feasibility of performing the role successfully in an alternative environment. A telecommuting arrangement is most appropriate for a position that has clearly defined tasks, measurable work activity, and does not require the employee to be present in the office during all normal business hours. Based on business necessity, a manager may decide not to permit telecommuting.

All telecommuting arrangements will be made for a set period of time as determined by the employee and their manager. Permission to telecommute can be handled on an ad hoc, short-term (up to 3 months), or long-term (3-12 months) basis. For short or long-term arrangements, managers and employees must consult with the Human Resources Benefits Department to formalize the arrangement. A completed Employee Telecommuting Request form (see appendices) must be completed for short and long-term arrangements. Short and long-term telecommuting arrangements require manager and VP/Dean approval. A telecommuting arrangement may be extended upon review by the manager and employee in consultation with Human Resources Benefits.

Telecommuting employees remain obligated to comply with all University policies and procedures. Consistent with the University's expectations of asset, data and information security for employees working onsite, telecommuting employees are responsible for ensuring university equipment is maintained to the same standards. This includes, but is not limited to, operating systems, antivirus/antispyware protection, and secured network access. Use of personal equipment in no way releases the university or employee from legal and administrative requirements set forth in its policies and procedures. Violation of such policies and procedures will result in termination of the telecommuting arrangement and possible disciplinary action.

A telecommuting arrangement is not an entitlement nor is it a right of employment. It is established at the discretion of the employing unit and may be subject to change at the unit's discretion.

A manager must consider the following when evaluating requests for a telecommuting arrangement:

- The telecommuting arrangement supports the department, college and university's goals, including cost effectiveness, excellent service, and high productivity.
- The impact of the telecommuting arrangement on the equitable work distribution, productivity, and communication needs among colleagues.
- Appropriate performance standards and measures will need to be in place.
- Established means of supervision, communication, and systems of accountability will need to be determined.

A manager must consult with Employee Relations if the telecommuting arrangement is being considered as an accommodation for a medical condition or disability.
Prior to requesting a telecommuting arrangement, employees must be familiar with the *Flexible Work Arrangements* and *Telecommuting* policies. Dependent care or personal responsibilities must be managed in a way that allows for successful meeting of job responsibilities. A telecommuting arrangement is not meant as a substitute for child/dependent care.

Performance and Productivity Metrics
Job performance will be evaluated in the same manner as it is when the staff member works in the office; however, managers and staff members are encouraged to establish and to evaluate productivity and performance standards for work completed while telecommuting. These measures should be detailed in a written document and may include quality and productivity measurements.
A telecommuting employee must maintain accurate time reporting, (including entering work time, vacation time, and sick time) appropriately and obtain prior management approval for overtime.

Attendance at on site meetings or events may be required as deemed necessary by the employee's manager

.

Workspace and Equipment

It is the telecommuting employee's responsibility to establish a space conducive to productive work and maintain a designated work space in safe condition.

Staff members must have a computer and internet access in order to telecommute. Staff members may use DePaul-provided or personal computer equipment to perform their jobs at home provided that all necessary software applications for the performance of their job are installed. If DePaul-provided equipment is used, maintenance must be performed by DePaul's Information Services. If staff member-owned equipment is used, all expenses are the staff member's responsibility. A staff member's manager determines whether to authorize DePaul-provided computer equipment.

Telecommuters are not eligible to receive DePaul-issued printers, fax machines, modems, copy machines or any other hardware. Telecommuters are expected to obtain and pay for installation and ongoing service fees for internet access. The university will not be responsible for operating costs, home maintenance, or any other incidental costs

The following technology related subjects must be addressed when determining a telecommuting arrangement. The guiding principle in establishing these guidelines is protection of DePaul confidential data, and required equipment and processes depend on the types of data the employee must handle. Refer to the *Information Security Policy* for definition of "DePaul covered data" and data classification and handling requirements.

DePaul covered data should not be stored on non-DePaul equipment, including commercial or cloud services or home file servers.

Equipment

There are four general categories of technology use that telecommuters may employ and the option chosen should have primary consideration for the type of data that the telecommuter works with.

1. Use of employee's personally owned or non-DePaul corporate owned computer

    - This option is most appropriate for those employees who telecommute only occasionally or who must perform DePaul functions from home on an emergency or ad-hoc basis.
    - DePaul covered data should not be saved to this computer, most especially those data considered highly sensitive.
    - In general, DePaul-licensed software may not be installed on this computer. (See http://software.depaul.edu for exceptions to this.)

2. Remote access to the employee's desktop/laptop at DePaul

- All remote access to a DePaul desktop access must be configured to encrypt network communications.
- The DePaul premises machine must be configured to the specifications provided at http://is.depaul.edu.

3. DePaul-owned Windows laptop/desktop

   - This option is the most preferable for regular and long-term telecommuting requirements.
   - Use of the computer should be limited to the telecommuter for DePaul business.
   - The computer should not be accessible via Windows remote desktop while being used off-campus.
   - This laptop must have the standard DePaul image and must be under active warranty. DePaul standard image will include these required attributes which must not be modified.
     - Computer is DePaul domain connected. (DePaul-imaged computers will remain connected to the domain unless the user takes purposeful action to remove it.)
     - DePaul's disk encryption solution (Bitlocker) must be on and the encryption key must be escrowed with DePaul
     - Computrace must be installed.
     - Centrally managed anti-virus software must be installed.
   - Telecommuter must use the DePaul virtual private network (VPN) while the computer is in use off-campus. Instructions on its use can be found at http://is.depaul.edu.
   - The first logon of the telecommuter to this machine must be performed on premises while the computer is attached to the DePaul network.
   - Data should most often be stored on DePaul network file servers (the U or W drive, depending on sensitivity level and sharing requirements).
   - If it is necessary to store data on the machine itself, all data should be backed up to the telecommuter's network U drive at least weekly.
   - The computer must be connected to the DePaul network on campus at least once every 30 days.

4. DePaul owned Mac laptop/desktop: This laptop must be under active warranty and have been through Information Services Mac setup procedures, wherein DePaul management software will be installed. The telecommuter must not modify or remove the DePaul management software.

   - The computer should not be accessible through remote access while being used off-campus.
   - All accounts on the computer must be set up with strong passwords (8 or more characters, with at least one numeral and one special character).
   - Encryption of the hard drive must be turned on. See http://is.depaul.edu if instruction is needed. The encryption key must be noted and escrowed with DePaul by emailing it to macencryption@depaul.edu along with the serial number of the computer.

- Telecommuter must use the DePaul virtual private network (VPN) while the computer is in use off-campus. Instructions on installation and use of the VPN can be found at http://is.depaul.edu.
- Data should most often be stored on DePaul network file servers (the U or W drive, depending on sensitivity level and sharing requirements).
- If it is necessary to store data on the machine itself, all data should be backed up to the telecommuter's network U drive at least weekly.
- The computer must be connected to the DePaul network on-campus at least once every 30 days.
- Mac users should consult IS before upgrading to the latest version of MacOS to ensure compatibility with needed systems and software.

DePaul Support

DePaul owned computers will be supported by DePaul IS via the Technology Support Center (TSC). Computers and equipment that are not owned by DePaul (e.g. home wifi routers, home printers or scanners, etc.) will not be supported by DePaul IS.

The TSC will provide phone support and will attempt to resolve the problem remotely. Any issues that cannot be addressed via the phone may require the return of the computer to campus for additional support.

Technology

Network:

The telecommuter will require a high speed Internet connection. If utilizing a home wireless network, the wireless network must be secured appropriately with WPA or better encryption and strong (12 character or better) non-default passwords.

VPN:

DePaul will provide access to a Virtual Private Network (VPN) that will allow the telecommuter to access their DePaul email, PeopleSoft and network drives via a secure encrypted connection.

Direct database access will not be available. Anyone that requires access to additional, specialized resources from off-campus will need to contact Information Security via the Technology Support Center.

Backup and DePaul Data:

DePaul data must remain secure. It is recommended that DePaul data be maintained on DePaul file servers (W and U drive). If it is necessary to keep data locally, the data should be backed up to the U drive on at least a weekly basis. If sensitive DePaul information is to be retained on paper, the telecommuter must have appropriate locking cabinets and a shredding device.

Policies:

The following University policies apply to DePaul University computers:

Acceptable Use Policy/Network Security

Access to and Responsible Use of Data

Telephone

DePaul telephone service is not available at remote locations. Telecommuters must use a cell phone or privately-owned land line.

Call forwarding from a DePaul telephone extension is also not available.

The DePaul voice conferencing service is not available from off-campus. See Procurement's web site for commercial alternatives.

Safety and Accidents

The alternative work site is subject to physical inspection by DePaul University and any agents on behalf of DePaul University. A telecommuting employee must agree to comply with any such request. In order to maintain data privacy and integrity, telecommuting work must be conducted only at a pre-approved work site. Business visits or meetings at the alternative work site are prohibited without approval of the employee's manager.

The telecommuting employee is responsible for insuring all equipment, not owned by DePaul University, used for telecommuting. The University will not be responsible for operating costs, home maintenance, property or liability insurance, or other incidental expenses (utilities, cleaning services, etc.) associated with the use of the employee's residence.

The employee shall not permit other persons to utilize the dedicated work space during business hours. The employee is liable for any injuries sustained by visitors to their work site. He/she must comply with all safety policies and procedures, including immediately reporting injuries sustained during working hours to his/her manager. Refer to the *Insurance Claims - University Property and Liability Policy* for additional information.

Pay and Benefits

The staff member's compensation and benefits are not affected by telecommuting. Telecommuters are responsible for determining federal, state and local tax implications resulting from working at a telecommuting location since tax withholding may be impacted when staff members telecommute from a different state than their work location state.

Procedures

Refer to the Employee Telecommuting Request form and the Telecommuting Guidelines and Procedural Checklist for Managers.

A telecommuting arrangement can be discontinued by management with a four week notice, though an immediate and unanticipated operational need may require the immediate suspension of the telecommuting arrangement. The dissolution of a telecommuting arrangement by a manager should be based upon employee performance or the operational needs of the work unit, and the rationale should be communicated to the employee in writing. An employee may request that the arrangement be discontinued. The granting or denial of such a request, and the timing of implementation if granted, is at management's discretion, based on business and operational needs.

Divisional Collaborations

Information Services

Contact Information

Office of Human Resources

Mailing Address:

1 East Jackson Boulevard
Chicago, Illinois 60604

Office Location:

14 East Jackson Boulevard
13th Floor
Chicago, Illinois 60604

(312) 362-8500

Appendices

Flexible Work Arrangements

Employee Telecommuting Request Form

Telecommuting Guidelines and Procedural Checklist for Managers

History/Revisions

Origination Date: 07/01/2014
Last Amended Date: 08/30/2017
Next Review Date: N/A