Non-faculty Telework Agreement Form for the COVID-19 Emergency

Employee Name: _____ Date: _____

☐ District Office ☐ Continuing Education ☐ ECC ☐ IVG ☐ MCC

Telework Location Address: _____

_____

Employee Contact Phone Number: _____

Emergency Contact Name: _____ Phone Number: _____

Purpose:

The purpose of this telework agreement is to provide parameters for non-faculty employees using telework during this emergency situation. Agreeing to telework requires a stable internet connection at home or suitable alternative location approved by your supervisor and unit head.

This agreement is only in effect during the COVID-19 emergency as declared by the District. During assigned scheduled hours of work, employees will need to be available to the supervisor. Failure to be available may result in disciplinary action up to and including discharge. The telework location you identified above is considered your assigned work area. Supervisors will monitor employee performance during assigned scheduled hours of work.

Employees working away from campus are expected to:

- Continue to satisfy the requirements of their position;
- Prioritize work to meet deadlines;
- Meet performance expectations as they would if working on campus;
- Adhere to all IVCCD policies and procedures related to employee conduct, workplace injuries, time and absence, proper use of district equipment, etc. which apply in the remote work environment;
- If you have a dependent who requires active care, arrange for dependent care so that you can work uninterrupted during your scheduled work hours.

Work Hours:

The standard hours of work are 8:00 a.m. to 4:30 p.m. with a thirty (30) minute lunch break, Monday-Friday unless a different work schedule is agreed upon and noted here:

_____

Approvals will be made on a case-by-case basis only if it is in the best interest of the District and employee. There may be circumstances requiring on-site attendance during this period.

Employees are expected to follow IVCCD policies on leave usage if not working on a given day or days during this agreement.

Communication:

Teleworkers must keep their supervisor informed of progress on assignments worked on at home, including any problems they may experience while teleworking. The employee will promptly notify the supervisor when unable to perform work assignments due to equipment failure or other unforeseen circumstances.

Teleworkers must notify their supervisor if they experience either Intranet or Internet failure for over 30 minutes.

Acceptable methods of communication specific to remote work include, telephone, email, Teams chat, and Zoom.

District-Owned Equipment:

As part of the telework agreement, District-owned equipment (including computers, docking stations, software and other telecommunications equipment) may be used by employees in their private residences, provided the property is used exclusively for official District business.

The District will retain ownership and control of hardware, software and data in all situations. Only software approved by the District will be installed on District-owned computers. The employee's supervisor and IT must approve any additional software before installation.

If District-owned equipment and/or software is damaged or malfunctions it must immediately be reported to a supervisor. If the District-owned equipment and/or software is damaged by non-employees (e.g., relatives or occupants of/visitors to the employee's household), the employee may be liable for all repair costs or replacement.

District-owned equipment is not for personal use at any time.

List equipment, software, and system access needed to perform required tasks (computer, phone, network drives (H drive), EX, Blackboard, Lumens, etc.) here:

_____

_____

Security:

Employees must comply with the District's security policies and procedures and ensure adequate security measures are in place to protect the equipment and information housed or

stored on assigned computers. Failure to comply with security policies and procedures may be grounds for disciplinary action.

Employees must keep all personal identifiable information confidential.

Employees granted VPN access must comply with the following requirements.

- VPN access is ONLY allowed on District-owned equipment.
- It is the employee's responsibility to ensure that unauthorized users do not have access to the District's internal networks or confidential information.
- VPN credentials are issued to a single individual and may not, under any circumstances, be shared.
- VPN gateways will be set up and managed by the District's IT department.
- All computers connected to the District's internal networks via VPN must be using up-to-date anti-virus software.
- While connected to the District's VPN, employees will limit their activity to mission-related traffic, refraining from personal email or web traffic.

Is VPN access required? ☐ Yes ☐ No If so, how will VPN access be utilized?

_____

I understand that I must comply with relevant policies and compliance including data security and confidentiality, intellectual property, equipment liability, and records retention.

I agree to the terms of this telework agreement. I understand this agreement is only in effect during COVID-19 emergency situation as declared by the District.

The duration of this agreement will be defined by the COVID-19 response period. IVCCD reserves the right to recall an employee back to campus work or require the use of leave if the telework is not productive.

Employee Signature_____ Date _____

Supervisor Signature_____ Date _____

Unit Head Signature_____ Date _____