Section: **E** Policy Number: **E-022** Subject: **Working From Home Policy** Total Pages: **5**	Approval Date: **June 17, 2020**

WORKING FROM HOME POLICY AND PROCEDURES

The intent of the Working from Home Policy and Procedures is to address the potential need to facilitate flexible working arrangements for Community Living-Central Huron employees in the case of exceptional circumstances **(**e.g. pandemic, widespread disease or disaster). Accordingly, the Policy shall not constitute a change to Employees' existing Letters of Employment, or provide any expectation and/or set a precedent that these arrangements will become permanent at some time in the future. The goal of the Policy is to protect the safety and well being of all Employees and continue to provide quality services and supports to people supported by Community Living-Central Huron. Due to Community Living-Central Huron's operational requirements, it is not possible to consider working at home arrangements for all employees. Therefore, should a position be deemed operationally essential by the Employer, the usual work arrangements/work locations will continue. Where it has been determined by the Employer to be in the best interests of the Employee, Agency and people supported to work from home, the Employee will be notified in writing, and will continue to be bound by all of Community Living-Central Huron Policies and Procedures. This Policy is not intended to eliminate the responsibility for which some staff may have with respect to addressing immediate support issues/concerns with people supported. Non-compliance with this Policy is subject to discipline, up to and including dismissal.

Definitions:

Exceptional Circumstances: situations that could not be reasonably foreseen or expected; insufficient time to take necessary action to resolve the situation arising from those circumstances. Examples**:** serious occurrences, epidemic, pandemic, services disturbances/disruptions or widespread disease or disaster such as severe weather events that last for several days, ie. Tornadoes, flooding, wild fires.

Telecommunications: for the purpose of this policy, telecommunication will be defined as tablets laptops, iPad, telephone, cellular and computer networks and the internet.

The granting (as well as the termination) of any such telecommuting privileges will be made in the sole and absolute discretion of the Board of Directors in consultation with the Executive Director taking into account the following:

1. the current status of exceptional circumstances as defined above;
2. the ongoing operational requirements of the Employer; and
3. the operational requirements of a particular role.

In certain cases, telecommuting arrangements may be granted subject to certain additional conditions and/or requirements owing to the particular role or circumstances.

All Employees operating under this Policy agree to remain bound by the following conditions and for the duration of their telecommuting arrangements:

- All internet connections used to access Employer related servers, email and information must be privately owned, password protected and have Wi-Fi connections that are not shared, nor publicly accessible;

- All work and employer related information, documents and email should be safeguarded from disclosure where in print, digital or other forms to family members, relatives, friends or members of the public, and regardless of whether the Employee deems such information to be confidential or not;

- All existing responsibilities and performance targets shall continue and where necessary, roles and responsibilities will be reasonably adapted in order to be continued under this Policy;

- All employees shall also remain available and accessible during ordinary business hours; and

- All other terms and conditions or employment, policies and procedures shall remain in place and their application adapted accordingly.

Community Living-Central Huron maintains their concern for the health, safety and liability of employees and the confidential and private nature of information. Therefore, Employees are required to, on an ongoing basis to take all reasonable and necessary precautions to safeguard their workspace, ensuring at all times that it is fit for the purpose of conducting work and is compliant with health and safety requirements. It will be the Employee's requirement when working from home to identify and remove all potential hazards from their workspace.

Employees who work under this Policy acknowledge and agree that despite the flexible nature of their work arrangements, they will not have any expectation to privacy in relation to Employer-owned electronic devices issued to them for the purposes of telecommuting work arrangements, including but not limited to computers, tablets, laptops, iPads and cell phones, and notwithstanding the fact that these will be used within the Employee's own residence and for Community Living-Central Huron business only.

Computers, tablets, iPads, laptops and cell phones, along with the contents of such devices, including but not limited to files, data, accounts, emails, messages, file systems and storage media that may be contained therein, whether in virtual or physical form will remain the property of Community Living-Central Huron at all times, and could be subject to inspection and/or repossession by the Agency at any time. The Employee acknowledges that they will not be entitled to retain possession of, or deny access to, any of the Employer issued equipment owing to the fact that the Employee has loaded personal information thereon. Conduct of this nature will constitute a breach of this Policy and may result in disciplinary action, termination for cause, and police intervention in circumstances that involve theft of Employer property.

Employees are also required to ensure that no other family member, relative, employee or third party has access to, or uses their Employer issued equipment and that all computers, tablets, iPads, laptops and phones are password protected and placed into a locked state whenever the Employee leaves their respective work area. Employees are also obliged to ensure that all work product and information is backed up daily in accordance with the Employer's standard practices.

In the event of any data security breach or accidental access by any family member or third party, the Employee will be obliged to immediately contain the breach and inform Human Resources. No third-party technicians, other than those pre-approved by the Employer in writing, may work on, repair, update or modify in any way, any of the Employer issued equipment or software. Further, the Employer will not be liable for any financial costs associated with an Employee's decision to retain a third-party technician to conduct unauthorized repair on any Employer-issued device in the Employee's possession.

All Employer issued equipment must also remain online during working hours**,** as per written notification from the Employer and accessible remotely by the Employer. The Employee in carrying out this obligation will ensure that the Employer has continuous access to such equipment and intellectual property at all times, the ownership of which will remain with the Employer.

Employees working under this Policy acknowledge that any telecommuting work arrangements are a privilege and that the Employer reserves its right to amend or withdraw such privileges at any time it deems appropriate. In the event of any such revocation, the Employee agrees to immediately revert to their ordinary work arrangements/work locations. In such cases, all other terms and conditions of employment will continue to apply, save only the privileges under this Policy.

In the event of termination of the Employee's employment, the Employee agrees that the Employer may immediately revoke access to Employer issued accounts and equipment, without advanced notice to the Employee, and that all information contained therein will constitute property owned by the Employer. The Employee also agrees that in the event of termination of employment they will immediately return and make available all Employer issued equipment, and to return to the Employer all Employer related documentation and assets. In such cases, no copies, drafts or backups of any form may be retained by the Employee. These obligations will similarly apply in the event that the Employee is suspended, pending an investigation, etc.

Given the nature of telecommuting work and the potential tax implications thereof, the Employer will not involve itself with the tax affairs of any Employee, nor will it make any misrepresentations to the Canada Revenue Agency on behalf of any Employee.

This Policy shall not detract from any existing Agency Policy and Procedures that apply and in the event of any conflict between this Policy and any other, the policy which provides the greater protection to the Employer will take precedence.

Procedure:

1. A letter will be issued by the Executive Director to employees involved outlining the conditions of the temporary conditions of working from home, reporting requirements, Agency equipment issued, etc. The letter would also advise employees their home work locations needs to meet health & safety obligations and a place in their home that is private, free from distractions and provides confidentiality for telephone calls, virtual meetings and webinars.

2. The Immediate Supervisor will provide a schedule of the work days and times; it is expected employees to keep normal working hours, ie. 8:00-4:00; 8:30-4:30; Supervisor notification/approval is required for overtime and as appropriate for use of sick time, personal time and vacation days. It is important the Employer is knowledgeable as to when employees are working/not working from a health and safety perspective, as well as for

employee benefits purposes and WSIB coverage. Employees will be available for regular daily calls and work assignments on the days they are working from home. Supervisors will check in each day with the Employee working from home; the Employee will provide a summary of what they worked on that day, accomplishments and any challenges encountered. Timesheets can be submitted electronically to their Supervisor, signed by the Employee, by noon the Monday following the pay end.

3. Employees will be provided a list of what agency equipment they will have in their possession, for example a laptop, iPad and/or a cell phone; such equipment will be password protected; equipment is for work purposes only and to be locked down when not in use; employees will be responsible to reimburse the Agency for any costs related to damage, lost and/or stolen property. Employees will be required to sign out all Agency equipment on the designated form. Community Living-Centra Huron will provide training on Agency equipment to employees before they begin working from home and will identify who will provide technical support to employees while they are working from home.

4. Some important Do's and Don't's; this is not an exhaustive list:

Don't:

- use random or found USB drives, plugging in an unknown USB drive could introduce malware to your device;
- connect to public wifi, avoid doing sensitive work or making any financial transactions;
- over-share on social media, hackers can use personal details shared on line to commit fraud;
- fall for "rush" requests even if it indicates it is from the Board President, Executive Director, or Human Resources;
- open links, attachments or files from banks, CRA or WHO, Public Health Ontario, Health Canada, etc;
- download apps indiscriminately;
- participate in spoofing attempts appearing to be from Management Staff within the organization asking for funds to be directed to external third parties;
- engage in phishing attempts whereby it allows for account takeovers initiated after you have clicked on links found within fraudulent or malicious emails, text messages, etc.;
- take home paper copies of files and/or data; only those that you absolutely require for the tasks to be accomplished;

Do's:

- be disciplined, develop a schedule and stick to it.
- learn about phishing scams, pause before you click on links in email, messages or on social media; preview unrecognized or suspicious links by hovering over them, do not go any further if there is misspelling or other irregularities or if the link does not match the text. Examples of threats: phishing emails, robo-calls, text messages and other communications promising advanced access to covid-19 vaccinations and/or 'too good to be true items" in exchange for credit card and other personal information;
- verify messages, text or email by phone if you believe it could be a scam;
- if for any reason a computer file is used outside of the network, back it up;
- ensure wifi connection is secure; anti virus and security software is in place and updated;

- take precautions during non-working hours, lock down and password devices;
- improve the physical security by keeping doors locked, store laptops, tablets, iPads in locked drawers when not in use and save/return discarded paper files/data to the Central Admin Office for proper destruction;
- disinfect devices, files, pens, stapler, etc. you bring home, and prior to returning them to the Employer's work location; best practice is to leave pens, staplers and other such items at work, or at home, if you transfer such ensure you disinfect them;
- contact HR with all concerns or possible breaches related to telecommunications; this will allow the Agency to act quickly to minimize the damage and take further preventative action, this is also required by the Agency's Cyber Insurance Policy;
- take regular breaks; set up your workspace in an area that will allow you to concentrate on work, separate home and work as much as possible;
- consider your background when on a video conference, having a wall, pictures, posters that are appropriate as a representative of the Agency; don't include family photos or any such information that may provide your location or information about your personal life;
- remember the Agency has an EAP Program;

Related Polices:

- All Polices and Procedures.

Other Documents:

- Job Description