

## Remote Work Policy

### Policy Purpose

Standpoint's Remote Work Policy outlines the protocol for staff who work remote (outside of the Standpoint office).

### Remote Work Agreement

Office based staff will work remote when deemed appropriate or necessary by the Executive Director. Staff that need to conduct their work remotely must discuss and get approval from the Executive Director prior to working remote. The Executive Director will assess staff eligibility on a case-by-case basis.

### Remote Work Requirements:

To ensure that staff are successful in remote work arrangements, remote staff are required to:

- Have access to distraction-free workspace.
- Have internet connection.
- Dedicate attention to job responsibilities during work hours, 8am-5pm Monday-Friday.
- Be able to work with other staff of Standpoint to complete projects and trainings as required in a timely manner.
- Be accessible to coworkers during work hours through Accession Application, email, and Slack.

### Compliance with Policies

Staff while working remote must follow Standpoint's policies similar to office-based staff. Examples of policies all staff should abide by are (refer to Standpoint's Human Resources Policies and Procedure Manual):

- Confidentiality
- Attendance
- Data protection
- Employee Code of Conduct

### Equipment

Standpoint will provide staff with technology equipment that is essential to their job duties. Standpoint will also install VPN and other agency required software on agency issued laptops. All equipment is agency property. Staff must keep it safe and avoid misuse.

Specifically, employees must:

- Keep their equipment password protected.
- Store equipment in a safe and clean space when not in use.
- Follow all data encryption, protection standards and settings.
- Refrain from downloading suspicious, unauthorized or illegal software.