**Disclaimer**

The contents of this template are intended to convey general information only and not to provide legal advice or opinions. The contents should not be construed as legal advice. CurrentWare advises consultation with legal counsel and/or an attorney for advice and legal opinion on specific legal issues.

# Frequently Asked Questions - Computer Monitoring at **[ORGANIZATION]**

*This document is intended to answer the most anticipated questions that employees may have about your use of computer monitoring software.*

*As a part of your deployment process, you may want to share your answers to these questions with your employees. You may also want to solicit feedback from employees and managers to gather FAQs that are specific to your organization.*

## Why Is Computer Activity Being Monitored? How Will the Data Be Used?

**[ORGANIZATION]** will be using computer activity monitoring software from [CurrentWare](https://currentware.com/) to enforce policies, ensure that IT assets are being used safely and appropriately, optimize work processes, and improve our business intelligence.

We trust our employees to perform at their best and manage their time effectively. The monitoring software will **not** be used to micromanage employees, spy on their every move, or intentionally collect personal information for nefarious purposes.

CurrentWare cannot capture individual keystrokes or webcam feeds; it will instead monitor internet and application usage so we can collect the computer activity data we need to improve our understanding of how our workforce operates.

**Examples of how CurrentWare will be used:**

* **Network Performance:** Bandwidth usage will be monitored to ensure that bandwidth hogs without legitimate business use (e.g. Netflix, Twitch, Prime Video) are not harming network performance.
* **Employee Safety & Liability:** Known NSFW websites will be blocked. How the rest of the internet is being used will be monitored to ensure that accessible websites are safe and appropriate for the workplace.
* **Cybersecurity:** Application and internet use will be monitored for high-risk activities and unauthorized software (“Shadow IT”). Portable storage device activity will be monitored to track the flow of sensitive information and protect data against theft.
* **Productivity:** We trust our employees to manage their time effectively. We also recognize that occasional limited web surfing is beneficial to employee productivity. We will only address employee web browsing habits if they are accompanied by performance issues (or if browsing is in violation of policies).
* **Software Licensing:** We will monitor the frequency of SaaS and application usage to help anticipate licensing requirements, such as deprovisioning lesser-used software and consolidating redundant solutions.

**The data that is collected through the monitoring software will only be used for purposes that are compatible with those outlined in [PRIVACY POLICY].** Any employees or representatives of **[ORGANIZATION]** that use employee computer activity data for an unauthorized purpose for which it was collected will be subject to corrective actions.

For more information about how your computer activity data will be collected, used, and protected, please refer to **[PRIVACY POLICY].**

## Who Has Access to My Computer Activity Data? How is it Secured?

All of the data collected by CurrentWare’s monitoring software will be securely stored and protected in the same manner that we protect other forms of personal information. Please see **[DATA SECURITY POLICY]** for more information.

When using CurrentWare to monitor computer activity, the software and all of the data it collects is entirely within the control of **[ORGANIZATION].** CurrentWare cannot access your data directly, though sample reports may be shared with them for the explicit purpose of troubleshooting the software.

Employee computer activity data will be made available to employees and representatives of **[ORGANIZATION]** that have a legitimate business reason to review the data. This includes, but is not limited to, an immediate manager of the employee, human resources staff, and information technology (IT) staff.

**All employees and representatives with access to employee computer activity data are trained on their data security and privacy responsibilities as per [PRIVACY POLICY].**

## What Will the Computer Monitoring Software Track?

**This section will cover all of the activities that CurrentWare is capable of monitoring.**

The data that is specifically captured by each CurrentWare solution depends on the solutions installed and the tracking methods that are enabled during deployment. At the organization’s discretion, we may enable or disable some of these capabilities on an as-needed basis.

*The information contained here is for reference purposes only and is current as of June 2021.* For the most up-to-date information on CurrentWare products, please refer to their [Release Notes](https://www.currentware.com/support/release-notes/) or contact **[CONTACT].**

### [BrowseControl](https://www.currentware.com/browsecontrol/)

**Web Filtering Software**

* Logs of websites that have been blocked (optional feature for troubleshooting)

### [BrowseReporter](https://www.currentware.com/browsereporter/)

**Employee Computer Monitoring Software**

* Websites visited including URL, content category, timestamp, and browsing time
* Application usage including timestamps
* Bandwidth usage, including the source URL
* Remote screen capture, including screenshots
* Search engine queries
* The IP address of the client computer (disabled by default)

### [AccessPatrol](https://www.currentware.com/accesspatrol/)

**Device Control & Data Loss Prevention Software**

* Logs of inserted portable storage devices (USB, DVD/CD, Tape, SD Card, etc), scanners, webcams, printers, and mobile phones | [Learn More](https://www.currentware.com/support/which-devices-can-i-control/)
* Logs of allowed vs denied peripheral devices
* File operations to portable storage devices (files copied, created, renamed, and/or deleted to/from these devices)

### [enPowerManager](https://www.currentware.com/enpowermanager/)

**Remote PC Power Management Software**

* Timestamps of computer power states: Startup, shutdown, and sleep events
* Timestamped logon and logoff events
* Duration of logons

### Will My Personal Devices Be Monitored?

**No.** CurrentWare will only be used to monitor organization-owned IT assets. That said, if you remotely connect to an organization-owned workstation or use an organization-provided VPN your computer and network activity may be subject to monitoring.

## Can I See My Own Computer Activity Data?

In the interest of transparency, **[ORGANIZATION]** has created processes that allow our employees to access their computer activity data.

1. BrowseReporter includes an optional [End-User Reports](http://currentware.com/end-user-reports/) feature that allows employees to have on-demand access to a dashboard with their internet and application usage data. If you would like to have this feature enabled, please contact **[CONTACT].**
2. In addition, you can request to see your computer activity reports on request. To do so, please reach out to **[CONTACT]**. They will guide you on the reports that are available and provide you with a copy of your desired report.

## I Have Other Questions. Who Can I Speak To?

Employees with further questions about **[ORGANIZATION]**’s use of computer monitoring software can reach out to **[CONTACT]** for more information.