

JORVIK RADIO EMPLOYEE MONITORING POLICY

VERSION 1.1 - UPDATED 08.11.2023

Definitions

(Company) IT Assets

"IT Assets" refers to devices and services that are owned, or managed by Jorvik Radio (including, but not limited to, computers, servers, and other hardware found within Jorvik Radio's estate), or credentials / access issued by the company, including when such access is used on a personal device, including emails. Data / traffic sent via networks owned or managed by Jorvik Radio, such as Wi-Fi or LAN, should also be considered as in scope, including personal devices.

Employee

"Employee" collectively refers to any directors, officers, managers, employees, volunteers, other representatives, and agents including consultants and contractors associated with Jorvik Radio.

Monitoring

"Monitoring" refers to the practice of collecting user activity data on Company IT Assets. This data includes, but is not limited to, web browsing history, files downloaded, data input, network traffic, logons to corporate systems, interactions with data, peripheral device usage, data sent / received / downloaded, and information about any device.

Personal Use

"Personal Use" refers to an employee using a Company IT Asset for personal tasks (such as non-work web browsing and sending personal emails) or private conversations held in presence of Video & Audio Surveillance devices.

Personal Information

"Personal Information" refers to any data or conversations collected or recorded about / referring to an identifiable individual(s). This includes obfuscated data that, when combined with other information, could identify the individual(s).

Video & Audio Surveillance

"Video & Audio Surveillance" refers to surveillance by means of a device(s) that monitors and records visual images and / or audio of activities on company-owned / company-managed property. This is for the safety, support, and security of the company and for those who are lone working, as stated in Jorvik Radio's Acceptable Usage Policy.

Purpose of the Workplace Monitoring Policy

Jorvik Radio (the "company") is committed to maintaining a transparent and fair workplace. Through this Workplace Monitoring Policy, Jorvik Radio will communicate the company's intent to monitor its employees, provide information about the categories of data collected, inform employees about how their data will be secured and used, and clarify privacy expectations when using Company IT Assets.

This Policy contains references to the policies, procedures, and practices that will be followed by Jorvik Radio, its representatives, and any of its present or future subsidiaries when collecting, using, or disclosing the personal information of an identifiable individual that is a present, future, or former employee of Jorvik Radio.

Privacy Statement: Expectation of Privacy in the Workplace

This section will outline the privacy rights and expectations that employees of Jorvik Radio will have during their involvement with the station.

Monitoring employee usage is an essential part of enforcing company policies, maintaining a respectful work environment, and ensuring that Company IT assets are used safely and appropriately.

For that reason, outside of the rights granted by GDPR, employees must not expect privacy when using Company IT Assets. While all personal information collected by Jorvik Radio will be used fairly and appropriately as per this Policy, all activities that take place via Company IT Assets should be considered monitored. Video and Audio recordings, as a principle, will not be monitored without good reason - as defined later within this document.

Personal Use of Company IT Assets

Jorvik Radio recognises that its employees may occasionally desire to use Company IT Assets for personal tasks during their normal course of business. This may include non-work web browsing, making personal phone calls, or sending emails from personal / corporate accounts.

Occasional personal use is permitted, however, to the fullest extent of the law Jorvik Radio reserves the right to monitor personal use of Company IT Assets to the same extent that it monitors business use. Employees must operate under the assumption that anything on Company IT Assets is monitored and conduct themselves accordingly.

Surveillance

Video & Audio surveillance equipment is used on company premises to ensure that employees, guests, and Company IT Assets are kept secure from theft, vandalism and other forms of misconduct, and to offer support as / where necessary for technical issues and for lone working care.

Should misconducts or unlawful activity be discovered, the recordings captured by surveillance equipment will be used to the fullest extent of the law - including the possibility of disclosure to authorised third parties.

Where such surveillance equipment is used, the equipment will be made clearly visible and there will be notices indicating its presence.

Monitoring

Jorvik Radio monitors the activity of Company IT Assets to ensure that they are used in accordance with Jorvik Radio's Acceptable Use Policy. Where a specific individual is being monitored, the individual will be notified in advance.

Computer activity data may also be used to detect malicious or high-risk activities, monitor network performance, and prevent security incidents from occurring.

Prohibited Forms of Surveillance

To provide Jorvik Radio's employees with a reasonable degree of privacy on Company IT Assets, the following forms of surveillance are strictly prohibited unless there are exceptional circumstances and a legitimate business reason* to do so:

- Keylogging (recording individual keystrokes).
- Surveillance monitoring in private spaces such as bathrooms.
- Covert surveillance.
- Covert recording or streaming of webcam feeds.

Should circumstances require that any of the aforementioned prohibited forms of surveillance be conducted, the surveillance will be done in accordance with the privacy requirements of GDPR.

** This could include situations involving alleged illegal activity, misuse of equipment, vandalism or theft of company property.*

Policy Enforcement

Corrective actions may be taken with regards to violations of this Policy. Depending on the severity of the violation, corrective actions may include suspension, legal action, and / or dismissal.

FORMAL ATTESTATION

I HAVE READ AND UNDERSTOOD THIS DOCUMENT IN ITS ENTIRETY AND AGREE TO THE CONTENT AND PRINCIPLES LISTED HEREWITIN:

NAME: _____ DATE: _____ SIGNATURE: _____