

EMPLOYEE MONITORING POLICY

Editable transparent-monitoring template

IMPORTANT - LEGAL REVIEW REQUIRED This template provides general information and is not legal advice. Monitoring laws differ by country, state, industry, workforce and technology. Notice, consultation, consent, a lawful basis, union or works-council involvement, a data protection impact assessment, or other safeguards may be required. Have qualified privacy and employment counsel adapt this document to every location in which workers operate.

Organisation	[Full legal name]
Policy owner	[HR / Privacy / Legal / Information Security role]
Version and approval	[Version] [Approved by] [Approval date]
Effective / review dates	[Effective date] [Next review date]
Countries/regions	[List every worker location covered by this version]

How to use this template

- Replace every [bracketed placeholder] and delete all drafting notes before issue.
- Select only monitoring methods that are actually enabled and verify the software configuration.
- Create location-specific addenda where legal requirements differ.
- Complete the legal-review and transparent-rollout checklists in the appendices.
- Give workers the final policy and any required privacy notice before monitoring begins.

1. Purpose and principles

[Company legal name] ("Company") uses limited workplace monitoring for the specific purposes described in this policy. The Company aims to ensure that monitoring is lawful, necessary, proportionate, transparent and no more intrusive than reasonably required.

Monitoring information can lack context. It will not be treated as a complete measure of performance, commitment or conduct. Managers must consider role requirements, approved breaks, technical issues, accessibility needs and the worker's explanation before drawing conclusions.

2. Scope

This policy applies to [employees / contractors / temporary workers / other categories] working [remotely / in Company workplaces / on a hybrid basis] in [locations].

It applies to [Company-owned devices / managed work profiles / specified accounts and systems]. Personal-device monitoring is [not permitted / limited to the managed work profile described in the BYOD addendum].

3. Monitoring inventory

Complete the table with the exact production configuration. Do not leave a capability selected merely because the software supports it.

Use?	Monitoring category	Exact configuration / limits
☐ Yes ☐ No	Work time and attendance	[Hours, shifts, active tracker state; start/stop conditions]
☐ Yes ☐ No	Applications used	[Application name; whether duration and active status are recorded]
☐ Yes ☐ No	Work websites or URLs	[Domain only or full URL; exclusions for sensitive sites]
☐ Yes ☐ No	Active-window titles	[Fields captured; masking/exclusion rules]
☐ Yes ☐ No	Periodic screenshots	[Frequency, randomisation, blur/masking and pause controls]
☐ Yes ☐ No	Project and task activity	[Project selection, mapping rules and corrections]
☐ Yes ☐ No	Location or device information	[Specify precisely or mark not used]
☐ Yes ☐ No	Other	[Describe the data and collection method]

Expressly excluded monitoring: [for example, keystroke content, webcam capture, microphone/audio, continuous screen video, private communications or activity outside work time]. Any change requires documented legal/privacy review and any required advance communication or consultation.

4. When monitoring operates

Monitoring operates [during scheduled work hours / only while the approved desktop tracker is active / other exact trigger]. It is intended to stop [at shift end / when the worker pauses or exits the tracker / other].

Workers should protect personal activity by [using a separate personal device or profile / pausing or exiting the tracker / following another documented process]. If monitoring appears to continue unexpectedly, contact [support/privacy contact] immediately.

5. Defined purposes

The Company processes each category only for the selected and documented purposes below:

- [Accurate work-time and attendance records]
- [Project costing, resource planning or client billing]
- [Information-security and acceptable-use controls]
- [Workflow, capacity and process improvement]
- [Another specific purpose - avoid 'any business purpose']

The Company will not use monitoring data for an incompatible new purpose without completing applicable review, updating its documentation and giving any required notice.

6. Legal basis and required assessment

Applicable legal ground(s), as approved by counsel: [insert separately for each jurisdiction and purpose].

DPIA, privacy impact assessment or equivalent risk assessment: [reference, owner, approval date and review date / documented reason not required].

Consultation or representative involvement: [workers consulted / union or works council process / collective agreement / not applicable with documented rationale].

Drafting note: Do not assume that a worker's signature creates freely given consent. Employment relationships can create a power imbalance, and the appropriate basis depends on local law.

7. Notice and transparency

Before monitoring begins, affected workers will receive this policy and [the applicable employee privacy notice / monitoring notice / location-specific addendum]. The Company will explain:

- what data is collected and what is not collected;
- the purposes, operating schedule and device/account scope;
- who can access the data and how long it is kept;
- how monitoring data may affect decisions; and
- how workers can ask questions, correct inaccuracies or raise a complaint.

8. Access, use and manager responsibilities

Authorised access is limited to [roles] for [approved purposes]. Access is logged/reviewed by [role and frequency]. Managers must not browse monitoring information out of curiosity, share it informally, or use isolated activity signals as a substitute for fair performance management.

Monitoring records may be disclosed to [service providers / clients / professional advisers / regulators / law enforcement] only when [conditions and safeguards].

9. Retention and deletion

Data category	Retention period	Reason / deletion method
Screenshots	[e.g., __ days]	[Purpose and automated deletion]
App/website activity	[__ days/months]	[Purpose and deletion/anonymisation]
Timesheets/attendance	[__ years]	[Employment, payroll or tax basis]
Investigation hold	[Case-specific]	[Approval and closure review]

Data is deleted or irreversibly anonymised when its approved period ends unless a documented legal obligation, dispute or investigation requires a limited hold.

10. Security, providers and international transfers

The Company protects monitoring data using [role-based access, multi-factor authentication, encryption, audit logs, contractual controls and incident response]. Service provider(s): [name, role and link to privacy/security information].

Storage and transfer locations: [locations]. Transfer mechanism or safeguard where required: [details]. Security or privacy incidents should be reported to [contact/process].

11. Human review and significant decisions

Monitoring data may be incomplete, misclassified or affected by technical conditions. Before a significant performance, disciplinary or employment decision relies on monitoring information, the Company will verify relevant records, obtain meaningful human review, consider other evidence and give the worker a reasonable opportunity to explain context and challenge inaccuracies.

Solely automated decisions with legal or similarly significant effects are [not used / described here with counsel-approved safeguards and worker rights].

12. Worker rights, questions and complaints

Subject to applicable law, workers may ask what data is held about them, request access or correction, raise an objection, challenge a decision or submit a complaint. Contact: [HR/privacy lead, email, postal address and response process].

External regulator, worker representative, union, works council or grievance channels: [insert jurisdiction-specific details]. The Company prohibits retaliation for raising a good-faith concern or exercising a legal right.

13. BYOD, homeworking and private activity

Where personal devices are permitted, monitoring is technically limited to [managed work profile / approved application / work account]. The Company does not intend to capture private device use, household-member activity or personal communications. Workers should use [technical separation/process]. A Company device or alternative arrangement is available where [terms].

14. Investigations and covert monitoring

This general policy does not authorise covert monitoring. Any proposed exceptional monitoring must receive case-specific written approval from [Legal/Privacy/HR], satisfy applicable law, be limited in scope and duration, and include documented safeguards. Do not use this clause as operational authority without legal advice.

15. Accuracy, correction and context

Workers can report inaccurate time, project mapping, website/application classification, screenshots or other records through [process]. Corrections are reviewed by [role] within [timeframe], and consequential decisions are paused where appropriate until material disputes are resolved.

16. Training, audit and policy changes

Managers with access will receive training on privacy, security, contextual interpretation and fair decision-making. [Owner] will audit permissions, configuration, access logs, retention and policy accuracy every [period].

Material changes to purpose, data, technology, timing, access or decision use require renewed assessment and any legally required advance notice or consultation. This policy will be reviewed by [date/frequency].

17. Acknowledgement of receipt

I acknowledge that I received and had the opportunity to read this Employee Monitoring Policy and ask questions. This acknowledgement records receipt and understanding. It is not automatically consent, a contractual amendment or a waiver of statutory or contractual rights.

Worker name	[Full name]
Signature	[Signature or approved electronic acknowledgement]
Date	[DD Month YYYY]
Questions/notes	[Optional]

Appendix A - Legal-review checklist

- ☐ All worker locations and applicable employment, privacy and sector regimes are mapped.
- ☐ The exact production configuration and every data field have been inventoried.
- ☐ Purpose, necessity, proportionality and less intrusive alternatives are documented.
- ☐ A valid legal ground and any special-category condition are documented where required.
- ☐ DPIA/privacy impact assessment requirements are satisfied or the rationale is recorded.
- ☐ Advance notice, consultation, union, works-council and collective-agreement duties are satisfied.
- ☐ BYOD, homeworking, personal communications and household-member risks are controlled.
- ☐ Young-worker, biometric, health, union and other sensitive-data risks are excluded or reviewed.
- ☐ Provider contracts, security, subprocessors and international transfers are reviewed.
- ☐ Retention periods are justified by data category and technically implemented.
- ☐ Worker access, correction, complaint and human-review procedures are operational.
- ☐ The policy matches the final technical settings and manager permissions.

Legal reviewer: [name/firm] Jurisdiction(s): [list] Review date: [date] Approved version: [version]

Appendix B - Transparent rollout checklist

- ☐ Explain the operational problem and intended benefit before presenting the tool.
- ☐ Show workers exactly what is and is not collected using real configuration screens.
- ☐ Demonstrate start, stop, pause, break and personal-time controls.
- ☐ Provide the approved policy and privacy information before monitoring begins.
- ☐ Offer a real question, correction and grievance route.
- ☐ Train managers not to treat activity metrics as self-explanatory performance scores.
- ☐ Pilot with a representative group and document concerns and responses.
- ☐ Audit permissions, retention, configuration and access logs after launch.

Appendix C - Monitoring register

Data	Purpose	Source/timing	Access	Retention
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]

Authoritative starting points

Use current official sources and local counsel. These links are starting points, not a complete legal analysis.

- [UK ICO - Data protection and monitoring workers](#)
- [UK ICO - Specific considerations for monitoring methods](#)
- [Government of India - Digital Personal Data Protection Act, 2023](#)
- [Government of India - Digital Personal Data Protection Rules, 2025](#)

Final legal approval record

Reviewer	[Name / firm]
Jurisdictions reviewed	[List]
Approved version	[Version]
Review date	[DD Month YYYY]
Conditions / addenda	[List or attach]

Prepared by Backlsh | <https://backlsh.com/> | Template version 1.0 | 1 September 2026