Section 2.1. Digital Literacy and Ethical Immaturity in Digital Governance: An Integrated Competency Framework

Svitlana Greben[1]

[1]*Ph.D. (Public administration), Financial Research Analyst, Rating Agency "MIRA", Head of the budgeting department, State Enterprise «INFOTECH», Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-0432-9132*

Citation:
Greben, S. (2025). Digital Literacy and Ethical Immaturity in Digital Governance: An Integrated Competency Framework. In S. Breus (Ed.), *Digital Leadership in Education and Science: Navigating Innovation in the Age of Transformation.* 272 p. (pp. 90-117). Scientific Center of Innovative Research. https://doi.org/10.36690/DLES-90-117

This monograph`s chapter is an open access monograph distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC 4.0) license

OPEN ACCESS

Abstract. *Digitalization has transformed workplaces into socio-technical systems where ethical outcomes are produced through data collection, platform governance, algorithm-assisted decisions, and cybersecurity architectures operating continuously at scale. Ethical leadership therefore shifts from episodic moral intervention to an integrated governance capability that links values to enforceable controls, contestable procedures, and evidence of effectiveness. The main objective os to synthesize an integrated model of ethical leadership for digital organizations and to specify mechanisms, roles, workflows, and competencies that reduce predictable failure patterns, including function creep, opaque automation, responsibility diffusion, and trust erosion. A conceptual monographic synthesis is conducted using a systems perspective. The analysis specifies interdependent leadership functions, derives a minimal governance structure with explicit decision rights, translates oversight into lifecycle artifacts with go or no-go criteria, and operationalizes proportionality through risk tiering and a balanced measurement and assurance framework. Five interdependent governance functions are identified: normative and policy-oriented rule setting; techno-ethical governance through privacy by design, auditability, access control, and bias testing; human-centred protection of dignity, psychological safety, and sustainable performance, including boundary norms and the right to disconnect; air and inclusive participation via accessibility, accommodations, and capability building; and accountable and transparent governance that assigns responsibility, enables contestation, and sustains trust. Ethical leadership becomes credible when institutionalized as continuous governance integrated with HR, security, legal compliance, procurement, and enterprise risk management, supported by independent assurance and feedback loops. The proposed approach strengthens ethical reliability and operational resilience by making decisions traceable, reviewable, and improvable across the full lifecycle of digital tools. Future studies should validate maturity indicators across sectors, test intervention bundles in hybrid teams, and examine how generative AI reshapes due process, monitoring boundaries, accountability, and professional development.*

Keywords: *ethical leadership; digital workplace; socio-technical governance; privacy by design; algorithmic fairness; human-centred work; right to disconnect; data governance; cybersecurity ethics; contestability; accountability; maturity models.*

1. Ethical leadership as an integrated governance capability. Ethical leadership in the digital workplace increasingly functions as an organizational capability, not as episodic moral intervention by individual managers. This is because the most consequential ethical outcomes are now produced through system mediated processes, including data collection regimes, algorithm assisted decisions, platform rules, and security architectures that operate continuously and at scale. In such conditions, ethical intent must be translated into repeatable controls, explicit decision rights, and evidence that safeguards actually work under operational pressure. Ethical leadership therefore becomes a governance architecture that aligns values, policies, technical design, managerial routines, and cultural expectations into one coherent system. The integrated perspective is especially important because the major ethical domains interact, for example privacy conditions psychological safety, psychological safety shapes incident reporting, incident reporting affects cybersecurity resilience, and cybersecurity practices constrain responsible AI and HR analytics. A fragmented approach, where each domain is handled separately without shared accountability, tends to produce gaps, duplicated effort, and inconsistent messages that undermine trust. An integrated capability addresses this by clarifying functions, owners, escalation pathways, and verification mechanisms. The section below develops a deeper governance model built around five interdependent functions and the operating system that connects them.

The five function model conceptualizes ethical leadership as an interdependent system: a normative and policy oriented function, a techno ethical function, a human centered function, a fair and inclusive function, and an accountable and transparent function. Each function is necessary because it covers a distinct class of failure modes, yet none is sufficient alone because digital harms typically traverse boundaries. For example, a right to disconnect policy will not prevent burnout if performance management rewards constant responsiveness, and fairness commitments will not hold if data governance enables hidden function creep or biased inference. Integration is therefore not a rhetorical preference but a structural requirement for preventing predictable failure patterns. A well designed integrated model clarifies how principles become rules, how rules become system constraints, how constraints become routine practice, and how practice is audited and improved. This also supports legitimacy because employees judge ethical leaders not only by declared values, but also by whether protections are enforceable and contestable. In short, ethical

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

leadership becomes credible when it is institutionalized as a governance capability with continuous feedback loops.

To make the five function architecture concrete, it is useful to describe each function in terms of its purpose, typical instruments, and failure modes it prevents. The table 2.1 provides this functional specification and illustrates why integration is required for system level reliability.

Table 2.1. Five interdependent functions of ethical leadership in digital organizations

Function	Core purpose	Typical instruments	What it prevents if implemented well
Normative and policy oriented	Translate values into enforceable rules and procedural rights	Policies, standards, consent procedures, retention schedules, due process rules	Arbitrary decisions, ambiguous consent, uncontrolled secondary use
Techno ethical	Encode ethical constraints into design, procurement, and audits	Privacy by design, model governance, bias audits, access controls, logging	Function creep, opaque automation, non verifiable vendor claims
Human centered	Protect dignity, psychological safety, and sustainable performance	Right to disconnect, work design norms, supportive management practices	Burnout, chilling effects, moral injury, micromanagement cultures
Fair and inclusive	Ensure equal opportunity to participate and be evaluated fairly	Accessibility standards, training, accommodations, equitable workflows	Digital divide, structural exclusion, visibility bias, proxy discrimination
Accountable and transparent	Assign responsibility, enable contestation, and sustain trust	RACI, escalation paths, incident disclosure, appeals, reporting	Responsibility diffusion, silent harms, legitimacy crises

Source: developed by the author

The functional specification shows that ethical leadership is not a single competency but a composite system in which rules, technologies, management practices, inclusion mechanisms, and accountability must cohere. If one function is weak, harms tend to leak through the gap, often with delayed detection. Integration therefore serves as a reliability strategy that reduces both ethical drift and operational instability.

Integration depends on an operating model that defines who decides, who advises, who implements, and who verifies. Without explicit decision rights, ethical governance is often reduced to informal influence, and harms are later explained as unavoidable side effects of technology. A robust operating model assigns ownership to roles that have authority to pause deployment, require remediation, or reject high risk tools when safeguards are not credible. It also establishes cross functional forums that review high stakes deployments, such as HR AI, monitoring expansions, and new data

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

integrations. Importantly, governance forums should be designed to reduce symbolic compliance, meaning they require evidence, documented alternatives, and risk proportionality rather than broad assurances. The operating model should also protect employee voice by including representative perspectives or structured consultation, since many harms are first detected by those exposed to them. Finally, integration requires a clear interface between ethics governance and existing risk systems, such as information security, legal compliance, HR, and enterprise risk management, so that ethics is not treated as a parallel bureaucracy.

Because accountability frequently fails through role ambiguity, it is useful to define a minimal governance structure that can be adapted to different organizations. The table 2.2 proposes a practical role set and clarifies responsibilities that support integrated ethical leadership.

Table 2.2. Minimal governance structure for integrated ethical leadership

Role or body	Primary responsibilities	Decision authority	Typical outputs
Executive sponsor (senior leader)	Sets priorities, ensures resources, resolves conflicts	Can pause or reprioritize major deployments	Ethics governance charter, annual priorities
Digital ethics and governance committee	Reviews high risk tools, approves safeguards, monitors evidence	Approves, rejects, or requires remediation	Impact assessment decisions, control requirements
Data protection and privacy lead	Minimization, retention, consent, access governance	Can block non compliant data practices	DPIAs, retention schedules, access reviews
HR governance lead	Fair HR processes, contestation, training for HR AI use	Can pause HR AI use and require human review	HR AI policy, appeal process design
Security lead	Cybersecurity controls, incident response, monitoring boundaries	Can enforce security controls and incident protocols	Security control reports, incident post mortems
Inclusion and accessibility lead	Accessibility by design, accommodations, capability building	Can require remediation before rollout	Accessibility assessments, training plans
Internal audit or assurance function	Independent verification, control testing	Can escalate findings to executives	Assurance reports, remediation tracking

Source: developed by the author

The structure clarifies that ethical leadership requires authority as well as expertise, because safeguards fail when owners cannot enforce them. It also shows that integration is feasible with a small set of roles if responsibilities and escalation paths are explicit. In practice, this reduces the likelihood that ethics becomes advisory language without operational consequences.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

Ethical leadership becomes operational when it is embedded into standard workflows across the lifecycle of digital tools, from idea and procurement to deployment and continuous monitoring. Lifecycle governance is necessary because many risks appear after launch through shifting use cases, data drift, expanded access, and repurposing of metrics for disciplinary decisions. A lifecycle approach also supports proportionality by specifying higher scrutiny for high stakes or high intrusiveness systems, such as AI supported employment decisions and continuous monitoring. Effective workflows require documentation that is understandable to non specialists, since legitimacy depends on clear reasoning rather than technical opacity. They also require employee facing transparency at appropriate points, especially when surveillance or automated decision support affects rights and opportunities. Finally, governance workflows should feed into continuous improvement by requiring post deployment review, incident learning, and periodic revalidation of assumptions. This prevents ethics from becoming a one time approval step that is forgotten after implementation.

To operationalize leadership responsibilities across time, it is helpful to translate the five function model into a lifecycle workflow with required artifacts. The table 2.3 outlines a practical governance sequence that makes ethical oversight repeatable.

Table 2.3. Lifecycle workflow for integrated ethical governance

Lifecycle phase	Key ethical questions	Required artifacts	Go or no go criteria
Ideation and scoping	What is the purpose, and is there a less intrusive alternative	Problem statement, proportionality rationale	Clear purpose and necessity demonstrated
Procurement and contracting	Can the tool be audited, explained, and constrained	Vendor disclosures, audit rights, data handling terms	Auditability and restrictions contractually secured
Design and configuration	What data is collected, inferred, and retained	Data map, retention plan, access model	Minimization and access constraints enforced
Pre deployment testing	Does the system create disparate impact or unsafe incentives	Bias tests, usability checks, security assessment	No material unfairness, acceptable risk posture
Deployment and communication	Do employees understand use, rights, and contestation	Plain language notice, training plan, appeal route	Contestability and communication in place
Post deployment monitoring	Are outcomes drifting, and are harms emerging	Monitoring dashboard, audit logs, periodic review	Evidence supports continued use, remediation tracked

Source: developed by the author

The workflow demonstrates that ethics is a continuous governance practice that must be present before, during, and after deployment. It also provides clear stopping points where leaders can require redesign or non

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

deployment if safeguards are not credible. This strengthens legitimacy because decisions become traceable, justified, and reviewable.

Digital ethics governance must embody proportionality, because not all tools carry the same potential for harm. Routine office productivity tools may require baseline controls, while systems that influence employment outcomes or collect sensitive data require heightened safeguards. Proportionality also prevents governance overload by focusing attention on high stakes and high intrusiveness domains. A risk tiering model helps leaders choose the appropriate control set and review intensity based on factors such as consequence severity, reversibility, affected population size, and the degree of inference involved. Tiering also supports consistent decisions across units, reducing perceptions of arbitrariness and favoritism. Importantly, tiering should not be used to avoid accountability; rather, it should clarify what extra safeguards are mandatory as risk rises. A well embedded tiering approach improves both ethics and efficiency because it creates predictable expectations for project teams.

To implement proportionality, leaders need a simple risk tiering schema that links risk level to mandatory controls. The table 2.4 provides a practical tiering model that can be adapted to organizational context.

Table 2.4. Risk tiering and corresponding governance controls

Risk tier	Typical systems	Why risk is elevated	Mandatory controls (minimum)
Tier 1, baseline	Collaboration tools, standard analytics	Limited sensitivity and low consequence	Data minimization, basic access control, transparency notice
Tier 2, moderate	Productivity dashboards, limited monitoring	Behavior measurement and incentive effects	Retention limits, manager training, periodic review of impacts
Tier 3, high	HR AI decision support, continuous monitoring	Rights and opportunity impacts, inference at scale	Impact assessment, bias audits, explicit appeal routes, human review
Tier 4, very high	Emotion inference, biometric systems tied to employment decisions	Dignity risk, irreversibility, high misuse potential	Strong justification, independent review, strict prohibitions on punitive use, executive approval

Source: developed by the author

The tiering model makes proportionality actionable by linking risk characteristics to non negotiable safeguards. It also supports consistent leadership decisions across departments, reducing the chance that high risk tools are adopted through convenience or vendor persuasion. In practice, tiering strengthens both trust and governance efficiency.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

Ethical leadership in digital organizations must be assessed through evidence, because harms can remain invisible if leaders only track productivity outputs. Measurement should therefore include both control effectiveness indicators, such as retention compliance and audit completion, and human impact indicators, such as trust, psychological safety, and contestation outcomes. Importantly, metrics should avoid replicating surveillance logic; aggregated indicators and privacy preserving analytics are preferable to individual tracking. Assurance mechanisms are equally important because internal confidence can be biased, especially when those responsible for deployment also evaluate success. Independent testing, periodic audits, and documented remediation help convert ethical leadership into verifiable stewardship. Evidence also enables learning, since patterns in appeals, incident reports, and fairness monitoring can inform redesign and training priorities. Over time, high quality measurement strengthens legitimacy by demonstrating that leadership commitments are more than aspirational language.

To prevent ethical governance from becoming symbolic, leaders need a balanced evidence set that covers policies, technical controls, human impacts, and accountability performance. The table 2.5 proposes a compact measurement framework that can be reported periodically.

Table 2.5. Evidence and metrics for ethical leadership governance

Evidence category	Example metrics	What the metrics indicate	Common failure signal
Policy adherence	Retention compliance rate, DPIA completion	Rules are implemented, not only written	Frequent exceptions without justification
Technical control effectiveness	Access review completion, audit log coverage	Systems enforce boundaries	Broad permissions and missing logs
Fairness outcomes	Disparate impact ratios, override patterns	AI and processes are not producing systematic inequity	Persistent gaps without remediation
Procedural justice	Appeal volume and resolution time, correction rates	Contestation is realistic and timely	Appeals ignored or overly slow responses
Well being and climate	Psychological safety scores, burnout indicators	Work is sustainable and voice is safe	Declining trust and reduced reporting
Accountability performance	Remediation closure cycle time, incident post mortem completion	Organization learns and corrects	Repeated incidents with no systemic change

Source: developed by the author

The framework reinforces that ethical leadership is measurable when it is defined through controls, outcomes, and responsiveness to harm. Balanced evidence reduces the risk that ethics is evaluated only through productivity

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

or compliance narratives. It also supports continuous improvement because leaders can identify where safeguards fail and allocate resources accordingly.

Organizations rarely begin with a fully integrated ethical governance capability. More commonly, they evolve from ad hoc responses to incidents, to formal policies, to systematic controls, and finally to ethical foresight embedded into strategy and design. A maturity model helps leaders identify the current state, prioritize next steps, and communicate progress realistically. It also clarifies that ethical leadership is not a static label; it is a developmental trajectory that requires investment in skills, governance routines, and cultural reinforcement. Mature systems tend to show consistent decision making, clear accountability, and fast remediation, while less mature systems show fragmented ownership and reactive crisis management. Importantly, maturity increases when leaders align incentives with ethical outcomes, for example by rewarding managers for sustainable workload practices and for responsible handling of contestations. The maturity view also supports credibility because it encourages transparent acknowledgment of limits and a structured plan for improvement.

To support practical implementation, a maturity model can translate the integrated framework into staged organizational capabilities. The table 2.6 outlines a four level maturity pathway with diagnostic characteristics and priority actions.

Table 2.6. Maturity model for integrated ethical leadership capability

Maturity level	Typical characteristics	Primary risks	Priority actions
Level 1. Incident-driven, non-systematic governance	Ethics addressed after incidents, inconsistent practice	Repeated harms, low trust, blame culture	Establish ownership, basic policies, incident learning routines
Level 2. Policy-centric, compliance-oriented governance	Policies exist, enforcement uneven, limited evidence	Symbolic compliance, function creep	Implement controls, retention enforcement, access reviews, training
Level 3. System-governed, evidence-based governance	Lifecycle reviews, audits, dashboards, clear escalation	Overreliance on metrics, governance fatigue	Improve proportionality tiering, streamline evidence, strengthen employee voice
Level 4. Foresight-oriented governance embedded in strategy	Ethics embedded in strategy and design, proactive prevention	Complacency risk, complex dependencies	Continuous revalidation, independent assurance, innovation with safeguards

Source: developed by the author

The maturity pathway clarifies that integrated ethical leadership is built through institutional learning and governance discipline, not through isolated

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

training or value statements. It also provides a realistic roadmap for moving from reactive controls to proactive ethical design. This supports sustained trust because improvements become visible in procedures, evidence, and outcomes.

Ethical leadership as an integrated governance capability rests on a simple but demanding premise: values must be converted into enforceable safeguards that operate at scale and remain valid under pressure. The five function model provides a coherent structure, but its effectiveness depends on an operating model that assigns authority, embeds lifecycle workflows, applies proportionality through risk tiering, and verifies performance through balanced evidence and independent assurance. The framework also addresses a core legitimacy challenge of digitalization, namely that opacity and asymmetry can make employees feel governed by systems they cannot understand or contest. By institutionalizing contestability, transparency, and accountable remediation, leaders protect dignity and fairness while maintaining the benefits of digital coordination and innovation. Finally, the maturity perspective emphasizes that ethical leadership is developmental, requiring continuous improvement rather than one time policy creation. In a digital workplace, ethical leadership is therefore best understood as organizational craftsmanship: the structured building of rules, systems, and culture that make responsible behavior the default path for both people and technology.

2. Operationalization: mechanisms, metrics, and everyday practices. Ethical leadership in a digital workplace becomes effective only when it is translated into routines that are observable, testable, and enforceable across departments and over time. The central operational problem is predictability: the organization must be able to apply the same ethical standards to new tools, new teams, and new vendors without relying on informal heroics or personal discretion. This requires mechanisms that connect values to decisions, decisions to technical and procedural controls, and controls to evidence that can be reviewed and improved. Operationalization also protects legitimacy, because employees judge ethics through lived experience, for example whether monitoring is bounded, whether AI decisions are contestable, whether downtime is respected, and whether incidents are handled transparently. A further requirement is proportionality, since governance that is too light enables harm, while governance that is too heavy becomes symbolic and is bypassed in practice. For that reason, operationalization should be designed as a minimal viable system of controls that scales by risk tier and produces auditable artifacts. In what follows, operationalization is structured across policy mechanisms,

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

process mechanisms, cultural mechanisms, and assurance mechanisms, with an emphasis on templates, workflow integration, and governance evidence.

Policy is operational only when it defines decision rights, thresholds, and procedural protections in a way that can be enforced by systems and verified by audit. Policies should therefore specify purposes, prohibited uses, retention limits, roles, and contestation pathways, rather than repeating aspirational values. In digital workplaces, the most common policy failure is ambiguity, such as broad permission to monitor "for productivity," undefined bounds on secondary use, or unclear rules about how AI outputs influence employment decisions. Another frequent failure is misalignment between policy language and platform configuration, which turns policy into a non binding statement. Policy mechanisms should therefore be designed alongside technical implementation requirements, with named owners and review cycles. Crucially, ethical leadership should treat high risk domains as requiring pre approval, not merely post hoc justification, especially for continuous monitoring, biometric identifiers, and AI supported HR decisions.

To make policy operational, leaders can standardize a small set of mandatory policy instruments that correspond to the highest risk domains.

Table 2.7. Policy instruments that operationalize ethical leadership

Policy instrument	Scope and trigger	What it must define to be enforceable	Minimum review cadence
Monitoring and privacy policy	Any workplace data capture about individuals	Purpose limitation, prohibited uses, retention, access roles, contestation procedure	Annual, and after major tool change
Algorithmic decision policy	AI used in recruitment, evaluation, promotion, retention	Decision role of AI, human review rules, explanation duty, appeal rights, bias monitoring	Semiannual for high risk uses
Right to disconnect and boundary policy	Hybrid work, cross time zones, high message volume roles	Downtime rules, after hours expectations, meeting governance, escalation for overload	Annual, and after reorganizations
Data governance policy	Any collection, storage, integration, retention of workforce data	Classification, minimization, retention schedules, lawful basis, access governance	Annual, and after incidents
Incident response and disclosure policy	Security incidents, data leaks, model failures	Disclosure thresholds, employee protections, remediation offers, learning requirements	After each major incident

Source: developed by the author

The table 2.7 lists these instruments, clarifies their scope, and specifies what "enforceable" means in practice. These instruments convert ethical commitments into enforceable constraints by specifying what is permitted,

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

what is prohibited, and how employees can contest outcomes. They also reduce ethical drift because policy review becomes a routine governance event rather than an exceptional reaction to crises.

Process mechanisms ensure that ethical questions are asked at the moment stakeholders can still change the design. This is the practical heart of ethical leadership because most downstream harms become expensive or politically difficult to correct once systems are deployed. In digital procurement, the ethical risk is often introduced through vendor opacity and contractual limitations that prevent audits or restrict transparency. In design and configuration, the primary risks are excessive data collection, permissive access, and default settings that silently expand surveillance or automation authority. In deployment, the key risk is legitimacy failure, where employees experience a tool as covert control because they do not understand what it does or how it affects them. Ethical leadership addresses these risks by requiring specific artifacts, by setting go or no go criteria, and by linking approvals to evidence rather than to assurances. Importantly, process operationalization should include off ramp rules, meaning clear conditions under which a tool must be paused, revalidated, or withdrawn.

Organizations benefit from a standardized set of artifacts that must exist before a digital tool can be approved, especially in high risk tiers. The table 2.8 lists practical artifacts that operationalize ethical review and make decisions traceable.

Table 2.8. Required artifacts for ethical review across the lifecycle

Phase	Required artifact	What it proves	Typical owner
Scoping	Proportionality rationale	Necessity and least intrusive alternative considered	Business owner with governance committee
Procurement	Vendor transparency packet	Auditability, limitations, data handling, model documentation	Procurement with Legal and Data governance
Design	Data map and access model	Minimization, access boundaries, logging feasibility	IT with Privacy and Security
Testing	Impact and bias assessment	Disparate impact risks and incentive effects evaluated	HR governance with Data science and Audit
Deployment	Plain language notice and training plan	Employees understand purpose, rights, and contestation	HR and Internal communications
Operation	Monitoring dashboard and review schedule	Ongoing evidence and trigger thresholds defined	System owner with Assurance function
Change management	Change log and re approval rule	Tool updates do not bypass safeguards	System owner with Governance committee

Source: developed by the author

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

When artifacts are standardized, ethics becomes a routine control system rather than an ad hoc debate. The organization also gains institutional memory, since each deployment leaves a documented trail that can be reviewed, audited, and improved.

Culture operationalizes ethics through everyday expectations, especially in hybrid work where norms are transmitted through digital behavior. Ethical communication must be specific enough to be actionable, which means explaining what data is collected, why it is collected, who can access it, and what rights employees have. Vague statements about trust or safety are insufficient when tools can infer behavior at scale. Role specific training is also essential because ethical risk is distributed unevenly across groups: managers make disciplinary and evaluation decisions, HR designs processes, engineers configure data pipelines, and employees are exposed to monitoring and platform rules. Training should therefore focus on scenarios, common mistakes, and decision thresholds, not only on rules. Managerial practice is the final link, because leaders can undermine policy through informal signals, such as praising constant availability or treating a system score as unquestionable. Ethical leadership requires managers to practice deliberation, document rationales for decisions, and invite contestation without retaliation.

A practical training model is to align modules with role based risk exposure and to define behavioral outcomes that can be observed.

Table 2.9. Role specific training that supports ethical digital governance

Role group	Core ethical risk exposure	Training focus	Observable outcomes
Line managers	Surveillance creep, micromanagement, automation bias	Proportional oversight, outcome based evaluation, handling contestations	Fewer punitive uses of weak signals, documented review rationales
HR professionals	AI fairness, due process, explanation duties	Bias awareness, appeal handling, human review protocols	Consistent explanations, timely appeals, reduced disparate outcomes
Data and IT teams	Minimization, access control, logging, model integrity	Privacy by design, secure configuration, audit readiness	Strong access boundaries, complete logs, fewer policy exceptions
Security teams	Duty of care, incident disclosure, monitoring boundaries	Ethical incident response, non punitive reporting, proportional monitoring	Faster disclosure, better reporting culture, reduced blame dynamics
Employees	Understanding rights, reporting concerns, boundary norms	Transparency literacy, safe reporting channels, boundary practices	Higher reporting confidence, appropriate tool use, less cynicism

Source: developed by the author

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

The table 2.9 offers a role specific curriculum that operationalizes ethical leadership competence. Role specific training is operationally superior to generic compliance modules because it targets the decisions that actually generate harm or prevent harm. It also improves consistency, since each role learns what responsible practice looks like in comparable situations.

Ethical metrics should be designed to detect drift, reveal uneven impacts, and trigger remediation before harms become irreversible. A common mistake is to use ethical metrics as a surveillance extension, which creates resistance and undermines trust. For that reason, metrics should be aggregated where possible, privacy preserving by default, and explicitly separated from disciplinary processes unless due process thresholds are met. Metrics should also be balanced across four domains: control effectiveness, fairness outcomes, procedural justice, and climate and well being. This balance prevents narrow optimization, for example excellent audit completion combined with worsening psychological safety, or low complaint counts that actually reflect chilling effects. Ethical leadership also requires setting trigger thresholds, since a dashboard without escalation rules becomes observational rather than corrective. Finally, metrics should be reviewed by a cross functional forum that can allocate resources and mandate change, otherwise data becomes a report with no effect.

To operationalize monitoring without creating a new surveillance regime, leaders can use a compact governance dashboard with aggregated indicators and defined triggers. The table 2.10 proposes a minimal dashboard structure with practical interpretation rules.

A balanced dashboard makes ethical leadership visible through trends rather than anecdotes. When triggers are defined, the organization moves from passive reporting to active correction, which is the decisive difference between ethical aspirations and ethical governance.

Performance management is a primary ethical lever because it defines what counts as success and which behaviors are rewarded. In digital workplaces, performance systems often drift toward what is easy to measure, such as online presence, message responsiveness, or tool usage, even when these proxies do not represent value creation. This drift creates predictable harms: metric substitution, gaming behavior, visibility bias against remote workers, and pressure to accept intrusive monitoring. Ethical leadership requires designing performance management around outcomes, quality, and collaboration, with explicit safeguards against proxy based evaluation. It also requires clarity about the role of digital signals, specifying when signals are advisory and when they can be used as evidence.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

Table 2.10. Ethical governance dashboard: indicators, meaning, and triggers

Indicator category	Example indicator	Interpretation	Trigger for action
Control effectiveness	Retention compliance rate	Whether data exposure is bounded over time	Any persistent exception trend requires remediation plan
Access discipline	Quarterly access review completion	Whether internal misuse risk is controlled	Low completion or repeated broad access approvals
Fairness outcomes	Disparate impact in hiring or ratings	Whether AI and processes produce unequal outcomes	Disparity above defined threshold triggers revalidation and redesign
Procedural justice	Appeal resolution time	Whether contestation is realistic	Delays beyond target trigger staffing or process change
Well being and climate	Psychological safety and burnout signals	Whether digital practices degrade trust and sustainability	Downward trend triggers workload and monitoring review
Boundary protection	After hours message volume aggregate	Whether always on norms are emerging	Sustained increase triggers policy reinforcement and manager coaching

Source: developed by the author

A further requirement is procedural fairness, meaning evaluations must be explainable, reviewable, and contestable. When leaders align performance management with human centered principles, they reduce incentives for surveillance and improve trust without sacrificing accountability.

Because evaluation systems often encode hidden values, leaders can use a design checklist that contrasts proxy based evaluation with outcome based evaluation. The table 2.11 clarifies design choices and their ethical implications.

Performance management can either reinforce ethical safeguards or undermine them by rewarding constant visibility and compliance behaviors. When outcome based evaluation becomes the norm, the organization reduces demand for intrusive monitoring and improves procedural justice in hybrid and algorithm mediated work.

Transparency is operational only when employees receive information in plain language at the moments it matters, such as before monitoring begins, when AI is used in a decision, or when a policy affects daily routine. Transparency should cover not only the existence of a tool but also its purpose, the data it uses, retention time, who can see outputs, and how employees can contest errors.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

Table 2.11. Performance management design choices and ethical implications

Design choice	Proxy based approach (high ethical risk)	Outcome based approach (lower ethical risk)	Governance safeguard
Visibility	Online presence as commitment	Deliverables and quality criteria	Documented expectations and review rubrics
Measurement	Tool usage equals productivity	Task impact and stakeholder value	Mixed evidence sources, contextual review
AI scoring	Score as final judgment	Score as advisory input	Human review required for high stakes
Feedback	One directional evaluation	Two way review with contestation	Appeal window and correction process
Pace	Continuous micro evaluation	Periodic evaluation with reflection	Limits on real time punitive interventions
Collaboration	Individual ranking	Team and cross functional contribution	Peer review with bias safeguards

Source: developed by the author

Many organizations fail here by publishing long policies that employees do not read, or by using technical language that does not clarify rights. Ethical leadership should implement a transparency pack, meaning a standard set of short documents and communication moments tied to the lifecycle of tools. A transparency pack also reduces rumor and cynicism because it makes leadership reasoning visible. It is especially important in sensitive areas such as monitoring, affective inference, and HR analytics, where secrecy is interpreted as hostile intent.

To make transparency consistent, leaders can standardize what content must be communicated and when. The table 2.12 proposes a minimal transparency pack that is easy to maintain and audit.

A transparency pack operationalizes dignity and procedural justice by making rights and boundaries understandable in routine work. It also strengthens governance because communication moments become auditable events rather than informal announcements.

Ethical leadership requires an improvement cycle that can respond to incidents, near misses, and evidence of drift without creating blame dynamics. Remediation should be time bound, visible, and linked to recurrence prevention, otherwise employees interpret governance as performative. Learning should be institutionalized through post incident reviews that identify system causes, such as incentive misalignment, unclear decision rights, or inadequate training, rather than focusing on individual fault. Assurance must be independent enough to detect blind spots, which is why internal audit or an assurance function is important for verifying control effectiveness. A further maturity feature is revalidation, meaning periodic

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

reassessment of whether tools remain necessary and whether their assumptions still hold as contexts change.

Table 2.12. Minimal transparency pack for ethical digital tools

Transparency element	What it must say	When it must be delivered	Why it matters
Purpose statement	Why the tool exists and what problem it solves	Before deployment	Prevents legitimacy failure and rumors
Data description	What data is captured and what is inferred	Before data collection	Supports informed understanding and trust
Access and retention	Who can view outputs and how long data is kept	Before deployment and upon change	Limits function creep and hidden power
Prohibited uses	What the organization promises not to do	Before deployment	Converts values into enforceable boundaries
Contestation route	How to appeal, correct, or challenge	At deployment and in onboarding	Ensures procedural justice is real
Change notice	What changed and why	Before major updates	Prevents silent expansion of surveillance

Source: developed by the author

Finally, improvement requires leadership willingness to pause or withdraw tools when harms persist, because credibility depends on visible restraint as much as on innovation.

To ensure that governance adapts over time, leaders can formalize a continuous improvement cycle with defined inputs, actions, and outputs. The table 2.13 presents a practical cycle that integrates ethics into organizational learning.

Table 2.13. Continuous improvement cycle for ethical digital governance

Cycle step	Input signal	Required action	Output artifact
Detect	Dashboard trigger, complaints, incident reports	Triage and classify risk tier	Triage log and owner assignment
Diagnose	Root cause analysis	Identify system causes and incentives	Post mortem or review report
Remediate	Control gap or harm confirmed	Redesign, retrain, reconfigure, or pause tool	Remediation plan with deadlines
Verify	After remediation	Test effectiveness and side effects	Assurance report and closure evidence
Revalidate	Periodic review	Confirm ongoing necessity and proportionality	Re approval or decommission decision

Source: developed by the author

A formal improvement cycle transforms ethical leadership from reactive crisis handling into disciplined stewardship. It also sustains trust,

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

because employees can see that concerns lead to concrete change, not only to communication.

Operationalization is the practical core of ethical leadership in the era of digitalization because it converts values into enforceable constraints, routine decision workflows, and evidence that can be reviewed and improved. Policy instruments create boundaries, but they become credible only when supported by lifecycle artifacts, role specific training, and performance management designs that reduce incentives for surveillance and proxy evaluation. Metrics and dashboards are necessary, yet they must be constructed to support learning and early detection rather than extending monitoring logic into governance itself. Transparency packs operationalize dignity and procedural justice by clarifying purpose, access, retention, prohibited uses, and contestation routes in plain language at the moments that matter. Finally, continuous improvement ensures that ethics remains adaptive as tools, vendors, and organizational conditions change. Taken together, these mechanisms form a practical operating system for ethical leadership that is measurable, auditable, and resilient under pressure.

3. Leadership competencies in the digital era. Ethical leadership under digitalization requires a competency profile that integrates ethical judgment with operational and technical literacy, because leaders are now responsible not only for interpersonal fairness but also for the socio technical conditions that shape decisions at scale. In digitally mediated workplaces, ethical harm often arises without overt intent, through default settings, vendor constraints, metric designs, and algorithmic inference that silently restructure autonomy and opportunity. Consequently, leaders must be able to evaluate what systems actually do, what they infer, and what they cannot validly conclude, since ethical appraisal depends on technical realism rather than on marketing claims. They must also practice disciplined proportionality, which entails choosing the least intrusive intervention that achieves a legitimate purpose and being able to justify that choice transparently. Just as importantly, leaders must sustain procedural justice, meaning that employees can understand how decisions are made, contest outcomes, and expect timely remediation without retaliation. Because ethical risk spans HR, IT, security, procurement, and operations, leaders must coordinate cross functional accountability and prevent responsibility diffusion. Finally, leaders must treat trust as a core governance asset that determines whether employees comply, report incidents, and cooperate with transformation rather than resisting it. The section below develops a deeper competency framework, connects competencies to observable behaviors, and proposes evidence based assessment methods.

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

A useful way to conceptualize leadership competence in digital ethics is to distinguish three layers: cognitive competencies, procedural competencies, and relational competencies. Cognitive competencies involve the ability to reason ethically about systems, understand trade offs, and detect flawed assumptions behind metrics or model outputs. Procedural competencies involve translating ethical reasoning into decisions, approvals, controls, and review routines that remain stable under pressure. Relational competencies involve building psychological safety, communicating transparently, and sustaining legitimacy when technology is contested. This layered view matters because many leaders possess strong values but lack procedural or technical capacity, which makes ethical leadership fragile and dependent on specialists whose incentives may differ. It also matters because in digital contexts, competence is demonstrated through choices about governance and design, not only through interpersonal tone. The framework below therefore treats competence as an organizational capability embodied by leaders, expressed through repeatable behaviors and verifiable artifacts.

To anchor competence in a coherent model, it is helpful to specify a structured competency architecture that leaders can use for self assessment, training, and performance evaluation. The table 12.4 presents a layered model with definitions and concrete manifestations in digital workplaces.

The layered model clarifies that ethical leadership is not reducible to moral intention, because leaders must also understand systems and operationalize safeguards. It also shows why competence gaps are predictable: cognitive, procedural, and relational layers fail differently and require different development interventions.

Digital literacy for leaders is not the ability to code, but the ability to grasp the functional logic and limits of socio technical systems sufficiently to govern them responsibly. Leaders must distinguish measurement from meaning, correlation from causation, and prediction from justification, since many ethical failures occur when predictive analytics are treated as authoritative explanations. They should understand that models can embed historical inequities, that proxies can re create sensitive attributes, and that accuracy can vary across groups, producing unfairness that is invisible without disparity testing.

Leaders also need literacy in data governance fundamentals, including minimization, retention, access control, and the difference between aggregated monitoring for system health and individual monitoring for discipline.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

Table 2.14. Layered competency architecture for ethical leadership under digitalization

Competency layer	Definition	What it looks like in practice	Typical failure when weak
Cognitive (ethical and technical reasoning)	Ability to judge ethical trade offs using accurate understanding of technology and context	Asks what data is inferred, challenges validity, identifies proxy risks	Accepts vendor claims, treats metrics as truth, overtrusts automation
Procedural (governance and control design)	Ability to translate values into enforceable routines and decision rights	Requires impact assessments, sets thresholds, enforces audits and appeals	Policies exist but unenforced, approvals lack evidence, drift after launch
Relational (trust and legitimacy building)	Ability to sustain psychological safety, transparency, and procedural justice	Communicates clearly, invites contestation, protects dissent	Chilling effects, fear of speaking up, cynicism about "ethics talk"

Source: developed by the author

Another core literacy domain is explainability and contestability, meaning leaders must know when a decision is too opaque to be ethically acceptable, especially in high stakes outcomes such as hiring, termination, or promotion. Finally, leaders must understand that tool performance changes over time due to drift, workforce changes, and shifting incentives, which is why ethical assurance is continuous rather than one time. Without this literacy, leaders are likely to substitute credibility narratives for verification and to delegate ethical accountability to technical staff or vendors, which increases risk.

Because "digital literacy" is often defined vaguely, leaders benefit from a clear set of literacy domains tied to governance obligations. The table 2.15 specifies what leaders must understand, why it matters ethically, and what questions they should routinely ask.

The literacy domains make clear that ethical leadership depends on the ability to ask accurate questions and demand verifiable answers. When leaders consistently apply these questions, they reduce dependence on persuasion and increase governance reliability.

Proportionality is a central ethical competence because digital tools make it easy to expand observation and control far beyond what is necessary for legitimate objectives. Leaders must therefore be able to justify why a particular monitoring regime is necessary, why less intrusive alternatives are insufficient, and how harm is minimized through design. Proportionality also requires attention to reversibility and misuse potential: a tool that collects biometric identifiers or infers emotional states carries inherently higher dignity risks than a tool that aggregates system performance data.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

Table 2.15. Digital literacy domains leaders need for ethical decision making

Literacy domain	What leaders must understand	Ethical relevance	Routine questions leaders should ask
Data lifecycle	Collection, inference, storage, sharing, retention, deletion	Prevents hidden exposure and function creep	What is collected, what is inferred, and what is the retention limit
Measurement validity	What signals can and cannot indicate performance or risk	Prevents unjust evaluation and metric substitution	Does this metric reflect quality and context or only activity
Algorithmic bias and proxies	How proxies reproduce discrimination and how disparities appear	Protects fairness and equal opportunity	Which groups could be disadvantaged and how will we test that
Explainability and contestability	Limits of black box decisions and what explanations are feasible	Protects due process and legitimacy	Can an affected person understand and challenge the outcome
Drift and feedback loops	How models degrade and how incentives reshape behavior	Prevents silent degradation and gaming	How will we monitor drift and perverse incentives post deployment
Vendor constraints	What vendors disclose, restrict, and control contractually	Prevents responsibility diffusion	Do we have audit rights and evidence of performance and limits

Source: developed by the author

Competent leaders should treat proportionality as a structured decision rule rather than as intuition, using risk tiering and pre defined thresholds for heightened review. They should also prevent normalizing high intrusiveness tools, since normalization can shift cultural baselines and erode privacy and trust even when direct harms appear limited. In operational terms, proportionality competence is expressed through disciplined scoping, clear prohibitions on secondary use, short retention horizons, and separation between security monitoring and performance discipline. This competence is also strategic because trust declines when employees perceive monitoring as convenience driven rather than safety driven.

To operationalize proportionality, leaders need a structured rubric that links justification, intrusiveness, and safeguards. The table 2.16 offers a practical proportionality assessment rubric that can be used when approving monitoring or analytics initiatives.

The rubric operationalizes proportionality as a repeatable control rather than a moral intuition. It also clarifies that high risk conditions are not automatically disqualifying, but they require stronger safeguards, clearer justifications, and more independent oversight.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

Table 2.16. Proportionality assessment rubric for monitoring and analytics

Dimension	Low risk indicator	High risk indicator	Required leadership response when high risk
Necessity	Clear safety or compliance need with evidence	Convenience or productivity narrative only	Demand alternatives analysis and tighten scope
Intrusiveness	Aggregated, non identifying data	Individual level continuous tracking	Limit to exceptions, implement strict access and retention
Reversibility	Easy to stop and delete data	Biometric or persistent identifiers	Require executive approval and independent review
Secondary use risk	Explicit prohibitions and enforcement	Broad "business purposes" language	Prohibit punitive use without due process and approvals
Consequence severity	No direct employment impact	Linked to discipline, pay, or promotion	Require human review, appeals, and documented rationales
Transparency	Plain language notice and consent clarity	Opaque or coerced consent	Strengthen disclosure, enable contestation mechanisms

Source: developed by the author

Deliberative decision making is an ethical competence because digitalization increases speed and reduces deliberation, making it easy for organizations to act on metrics without contextual judgment. Leaders must therefore protect space for reflection, dissent, and review, especially when decisions affect careers and livelihoods. Procedural justice is central in algorithm mediated work because employees assess fairness not only by outcomes but by whether the process is understandable, consistent, and contestable. A common ethical failure is "automation authority," where human reviewers treat system outputs as definitive, and individuals cannot obtain reasons or appeal effectively. Leaders should embed contestability by design, ensuring that decisions based on digital evidence have clear reasoning, documented thresholds, and appeal routes that are timely and safe. They should also create non retaliation norms so that contestation does not become career limiting. Procedural justice also includes correction rights, since errors in data can translate into unjust decisions if not corrected quickly. Overall, deliberation competence means leaders treat dissent as a risk detection resource, not as disloyalty.

Because procedural justice can be undermined by informal practices even when policies exist, it is useful to specify what contestability requires in operational terms. The table 2.17 defines contestability elements and the evidence that leaders should expect.

The table 2.17 shows that contestability is not a single channel but a system of explanations, review rights, corrections, and protections. Leaders

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

demonstrate competence when they maintain these elements even under time pressure and when they allocate resources to make them timely and credible.

Table 2.17. Contestability and procedural justice requirements for digital decisions

Procedural element	What it means	Why it matters ethically	Evidence leaders should require
Explanation duty	Provide understandable reasons, not only scores	Supports dignity and due process	Explanation templates, reason codes, communication logs
Human review	Consequential decisions require contextual judgment	Prevents automation bias	Review records, override logs, reviewer training completion
Appeal route	Accessible and safe channel to challenge outcomes	Makes fairness practical	Appeal tickets, time to resolution, outcome tracking
Data correction	Ability to fix inaccurate data quickly	Prevents persistent unjust effects	Correction workflow, correction time metrics
Non retaliation	Protection for those who contest	Sustains psychological safety	Policy enforcement cases, climate survey items
Consistency	Similar cases treated similarly with documented criteria	Reduces arbitrariness	Decision rubrics, calibration meeting notes

Source: developed by the author

Digital ethics is inherently cross functional because the same system may involve procurement contracts, data pipelines, security controls, HR processes, and managerial use in daily supervision. Responsibility diffusion is therefore one of the most common failure modes: HR assumes IT handles the tool, IT assumes HR owns outcomes, security focuses on threats, and no one owns the integrated ethical impact. Ethical leadership competence includes the ability to create shared governance structures with clear decision rights and escalation rules, as well as the ability to coordinate trade offs transparently. This competence also requires literacy in organizational incentives, since units may optimize for cost, speed, or compliance rather than for fairness and trust. Leaders must also ensure that ethics governance is not isolated from enterprise risk management, because ethical harms often become operational risks, such as turnover, litigation, reputational damage, and cybersecurity incidents. A key capability is to ensure that accountability is documented, meaning system owners are named and can be held responsible for monitoring, remediation, and revalidation. Where vendors are involved, leaders must ensure contractual audit rights and transparency obligations, otherwise governance cannot be evidenced. Cross functional competence is therefore a coordination skill grounded in formal authority and procedural discipline.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

To prevent responsibility diffusion, leaders can formalize accountability through a small set of standard responsibilities assigned across functions. The table 2.18 provides a practical mapping that links ethical domains to accountable owners and required coordination points.

Table 2.18. Cross functional accountability mapping for ethical digital systems

Ethical domain	Accountable owner	Consulted functions	Mandatory coordination checkpoint
Monitoring and privacy	Privacy lead	HR, Security, IT, Legal	Approval of scope, retention, prohibited uses
HR AI and fairness	HR governance lead	Data governance, Legal, Audit	Impact assessment and appeal readiness
Cybersecurity and duty of care	Security lead	IT, Legal, HR	Incident response readiness and disclosure protocol
Boundary protection	Line leadership with HR	Communications, Operations	Downtime rules and performance alignment
Inclusion and accessibility	Inclusion lead	Procurement, IT, HR	Accessibility validation before rollout
Vendor governance	Procurement with Legal	Security, Privacy, HR	Audit rights and documentation secured in contract

Source: developed by the author

The mapping clarifies that ethical leadership requires explicit ownership and predictable coordination points, not informal collaboration. When checkpoints are mandatory, ethical safeguards are less likely to be bypassed in fast deployments.

Trust building becomes a technical and governance competence in digital workplaces because employees often cannot directly observe what systems do with their data or how algorithmic decisions are produced. Trust therefore depends on credible transparency, consistent procedural justice, and demonstrated restraint in the use of monitoring and inference. Leaders must communicate purpose, boundaries, and rights in plain language, and they must close the loop by showing how concerns led to design changes or policy adjustments. Another key aspect is consistency: if leaders promise that monitoring is not used for discipline, but later use it opportunistically, trust collapses and future communications become ineffective. Trust is also shaped by whether leaders treat employees as partners in transformation, including involving them in pilots and consultations, rather than presenting change as inevitable. Importantly, trust is not the absence of control; it is the presence of legitimate control with clear limits and contestability. Ethical leaders therefore build trust through predictable processes, timely remediation, and visible accountability when failures occur. Over time, trust building competence becomes measurable through psychological safety

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

indicators, reporting rates for incidents and concerns, and the stability of boundary norms.

Trust is often discussed as a cultural ideal, yet it can be operationalized through concrete leadership behaviors and evidence artifacts. The table 2.19 connects trust building practices to what employees experience and to indicators leaders can monitor without increasing surveillance.

Table 2.19. Trust building practices and verifiable signals in digital workplaces

Trust building practice	What employees experience	Evidence artifact	Non intrusive indicator
Plain language transparency	Clarity about purpose and limits	Transparency pack, notices	Reduced rumor and complaint ambiguity
Demonstrated restraint	Boundaries are real and enforced	Prohibited use logs, retention audits	Stable trust items in surveys
Credible contestation	Appeals are safe and timely	Appeal records, resolution times	Increased reporting confidence
Visible learning	Problems lead to improvements	Post mortems, remediation plans	Fewer repeated incidents
Consistency across teams	Rules are not arbitrary	Governance checklists, calibration notes	Reduced perception of favoritism
Non retaliation protection	Speaking up is safe	Case reviews, policy enforcement	Higher psychological safety scores

Source: developed by the author

The table 2.19 demonstrates that trust can be built systematically when leaders align transparency, restraint, contestability, and learning. This is essential for ethical digitalization because employees' willingness to cooperate and report risks depends on perceived legitimacy.

Competency development should be treated as a governance investment rather than as optional training. Development is most effective when linked to role expectations and evaluated through evidence, such as the quality of proportionality rationales, the consistency of appeal handling, and the completeness of lifecycle artifacts. Leaders can build competence through scenario based training, simulations of incident response and contested decisions, shadowing governance reviews, and peer learning across units. Coaching is also important for managers transitioning from presence based supervision to outcome based leadership, as this shift is central to reducing demand for surveillance. Assessment should be multi source, combining audit evidence, team climate indicators, and review of decision artifacts, rather than relying solely on self reports. A mature approach also includes learning loops: incidents and near misses are used as training materials that improve future judgment and procedural discipline. In this sense, leadership

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

competence is not static; it is reinforced through continuous practice and organizational learning.

To institutionalize competence, organizations can align competencies with development interventions and assessment methods. The table 2.20 proposes a practical development matrix that connects what leaders must learn to how learning can be evidenced.

Table 2.20. Development and assessment matrix for ethical leadership competencies

Competency	Development intervention	Assessment method	Evidence of competence
Digital literacy for ethics	Scenario training on inference and limits	Review of tool approvals	High quality questions and justified constraints
Proportionality	Proportionality rubric workshops	Audit of monitoring scope changes	Reduced scope creep, documented alternatives
Procedural justice	Appeals and contestation simulations	Appeal performance metrics	Timely resolutions, consistent explanations
Cross functional accountability	Governance forum participation	RACI and checkpoint compliance	Clear ownership, fewer handoff failures
Trust building	Communication coaching and feedback loops	Climate indicators and feedback	Higher psychological safety, increased reporting confidence
Ethical foresight	Pre mortem and risk forecasting exercises	Post deployment review quality	Early detection of drift, proactive remediation

Source: developed by the author

The matrix shows that competencies can be developed and verified through practical interventions and evidence, rather than through abstract value statements. When assessment relies on artifacts and outcomes, ethical leadership becomes measurable and improvable over time.

Leadership competencies in the digital era can be understood as institutional craftsmanship: the ability to align values, systems, and culture so that responsible behavior becomes default rather than exceptional. Competence requires digital literacy that recognizes inference limits, proportionality that resists convenience driven intrusiveness, and deliberative practices that protect contestability and procedural justice. It also requires cross functional accountability to prevent responsibility diffusion and trust building to sustain legitimacy in opaque system mediated environments. The tables provided operationalize these competencies through observable behaviors, governance artifacts, indicators, and development pathways. As digital transformation accelerates, organizations will differentiate not only by technological adoption but by their capacity to

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

govern technology ethically and credibly. Ethical leadership competence therefore becomes a strategic capability that supports resilience, fairness, and sustainable performance in digitally mediated work.

Conclusion. The section demonstrates that ethical leadership in a digital organization should be treated as an institutional capability rather than as isolated moral decision-making by individual managers. This capability logic is justified by the fact that the most consequential ethical effects are increasingly produced by continuous, system-mediated processes such as data capture, algorithm-supported decisions, platform rules, and security architectures, which require enforceable controls and verifiable evidence of effectiveness. The five-function model provides a coherent architecture for integrating normative rule-setting, techno-ethical design and audits, human-centred protections, inclusion mechanisms, and accountability with transparency and contestation. Importantly, the text shows that integration is a reliability requirement: weaknesses in one function predictably "leak" harms into other domains, for example when well-being policies conflict with incentive systems, or when fairness claims collapse under weak data governance and hidden secondary use.

The operational contribution of the section is the translation of this architecture into a minimal but actionable operating model: explicit decision rights, cross-functional governance roles with authority to pause or remediate, lifecycle workflows with required artifacts and go or no-go criteria, proportionality through risk tiering, and a balanced evidence system that combines control effectiveness, fairness outcomes, procedural justice, and trust and well-being indicators. The maturity pathway clarifies how organizations typically evolve from incident-driven practices to foresight-oriented governance embedded in strategy, emphasizing that ethical leadership is developmental and must be sustained through audits, feedback loops, and learning routines.

Overall, the section positions ethical leadership as a form of socio-technical stewardship whose credibility depends on institutionalized safeguards, contestability, and continuous improvement rather than declarations of intent.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Brown, M. E., Treviño, L. K., & Harrison, D. A. (2005). Ethical leadership: A social learning perspective for construct development and testing. Organizational Behavior and Human Decision Processes, 97(2), 117–134. https://doi.org/10.1016/j.obhdp.2005.03.002
2. Eurofound. (2021). Right to disconnect: Exploring company practices. https://assets.eurofound.europa.eu/f/279033/50e4ba79e7/ef21049en.pdf
3. European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679
4. European Law Institute. (2023). Guiding principles on implementing workers' right to disconnect. https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Guiding_Principles_Workers_Right_to_Disconnect.pdf
5. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security management systems. https://www.iso.org/standard/27001
6. International Organization for Standardization. (2019). ISO/IEC 27701:2019 Privacy information management. https://www.iso.org/standard/71670.html
7. International Labour Organization & Eurofound. (2017). Working anytime, anywhere: The effects on the world of work. https://www.onlabor.org/wp-content/uploads/2017/03/wcms_544138.pdf
8. National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1
9. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
10. OECD. (2019). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449
11. Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020). Mitigating bias in algorithmic hiring: Evaluating claims and practices. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAccT '20). https://doi.org/10.1145/3351095.3372828
12. Ravid, D. M., White, J. C., Tomczak, D. L., Miles, A. F., & Behrend, T. S. (2023). A meta-analysis of the effects of electronic performance monitoring on work outcomes. Personnel Psychology, 76(3). https://doi.org/10.1111/peps.12514
13. UNESCO. (2023). Guidance for generative AI in education and research. https://unesdoc.unesco.org/ark%3A/48223/pf0000386693/PDF/386693eng.pdf.
14. W3C. (2023). Web Content Accessibility Guidelines (WCAG) 2.2. https://www.w3.org/TR/WCAG22/

https://doi.org/10.36690/DLES ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025

15. Walumbwa, F. O., Mayer, D. M., Wang, P., Wang, H., Workman, K., & Christensen, A. L. (2011). Linking ethical leadership to employee performance: The roles of leader-member exchange, self-efficacy, and organizational identification. Organizational Behavior and Human Decision Processes, 115(2), 204–213. https://doi.org/10.1016/j.obhdp.2010.11.002

https://doi.org/10.36690/DLES
ISBN 978-9916-9389-1-1 (pdf)
© Scientific Center of Innovative Research, 2025