

## **Initial Post: Codes of Ethics and Professional Conduct**

The ACM case study “*Abusive Workplace Behavior*” illustrates severe ethical and professional breaches by Max, a technical leader, and Jean, his manager. Max’s verbal aggression, gender-based retaliation, and denial of authorship contravene multiple principles of the ACM Code of Ethics, notably 1.1 (contributing to society and human well-being), 1.4 (being fair and not discriminating), 1.5 (honoring property and credit), and 2.2 (maintaining professional competence and integrity) (Gotterbarn et al., 2018). Jean’s failure to act ethically and protect staff dignity also breaches principles 3.3 and 3.4, as it perpetuates a psychologically unsafe environment (ACM, n.d.).

From a legal perspective, such conduct could violate employment law under UK and EU workplace harassment and equality legislation, including the Equality Act 2010, which prohibits gender-based discrimination and harassment. Furthermore, denying credit for research contributions may constitute a breach of intellectual property rights and employment contracts (Hughes et al., 2020).

Comparatively, the British Computer Society (BCS) Code of Conduct reinforces similar ethical imperatives, requiring members to “respect and value alternative viewpoints” (clause 2d) and to “not unfairly discriminate” (clause 1b) (BCS, 2021). Both codes emphasize professional integrity, accountability, and the duty to report misconduct.

The social implications of tolerating abusive behavior are profound—such cultures suppress diversity, creativity, and trust within teams. Professionalism in computing, therefore, extends beyond technical expertise to include ethical leadership and psychological safety. This case underscores the responsibility of computing professionals to foster equity, transparency, and mutual respect in all professional interactions (Johnson, 2020).

**Wordcount:** 243

## **References:**

ACM (n.d.) *Case Study: Abusive Workplace Behavior*. Available at: <https://www.acm.org/code-of-ethics/case-studies/abusive-workplace-behavior> (Accessed: 25 October 2025).

BCS (2021) *Code of Conduct*. British Computer Society. Available at: <https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/> (Accessed: 25.10.2025).

Gotterbarn, D., Miller, K. and Rogerson, S. (2018) ‘ACM Code of Ethics and Professional Conduct’, *Communications of the ACM*, 61(1), pp. 21–28.

Hughes, J., Monaghan, C. and Allen, D. (2020) *Employment Law for Business Students*. 3rd edn. London: Routledge.

Johnson, D.G. (2020) *Computer Ethics*. 5th edn. Harlow: Pearson.

### **Response Post 1:**

Thank you Jaco for your insightful contribution.

You raised important points about the ethical and technical responsibilities of medical implant startups under the BCS Code of Conduct. However, your discussion post could be expanded by considering how emerging regulatory frameworks and risk management methodologies are reshaping accountability in medical device innovation. Recent studies from Alberti et al. (2023) emphasise that ethical compliance now extends beyond technical reliability to include algorithmic transparency and AI interpretability in implantable technologies. This aligns with the European Union's forthcoming AI Act, which classifies medical AI systems as high-risk, requiring explainability and traceability (European Commission, 2024).

Moreover, scholars like Mittelstadt (2019) argue that developers should adopt *anticipatory governance*, integrating ethical reflection and stakeholder engagement throughout the research process, to mitigate long-term harms rather than relying solely on post hoc regulation. From a research methods perspective, this suggests that ethical risk assessment should be embedded into the design methodology itself, not treated as an external compliance task.

Therefore, while you rightly identify oversight and negligence, the broader issue concerns how organisations can embed ethical thinking proactively into research and innovation processes. This approach would help prevent harm before it occurs and support greater public trust in digital health technologies.

**Wordcount:** 202

### **References:**

- Alberti, M. et al. (2023) 'Explainability in Medical AI: Ethical and Technical Challenges', *AI and Ethics*, 3(1), pp. 45–60.
- European Commission (2024) *Artificial Intelligence Act: Regulation (EU) 2024/1689*. Brussels: Publications Office of the EU.
- Mittelstadt, B. (2019) 'Principles Alone Cannot Guarantee Ethical AI', *Nature Machine Intelligence*, 1(11), pp. 501–507.

### **Response Post 2:**

Thank you, Elias for your meaningful Initial Post on the topic of accessibility in Software Development.

You make an important point about how neglecting accessibility violates both ACM and BCS ethical principles. I agree that this is fundamentally a case of social exclusion, but I think the issue also reflects a broader organisational culture problem rather than just a failure of individual ethics. Recent work from González et al. (2023) highlights that accessibility is not only a moral or legal obligation but also a core

aspect of innovation and user experience. When inclusion is built into design from the start, it often leads to better usability for everyone.

It's also worth noting that international standards such as ISO 9241-210:2019 on human-centred design now treat accessibility as integral to product quality, not an optional extra. Ignoring these standards exposes companies to both reputational and economic risk (ISO, 2019). Furthermore, new research from Cech and Waidzunas (2021) in digital ethics suggests that accessibility should be viewed through the lens of digital justice, ensuring that technology development actively reduces social inequities rather than reinforcing them.

So while you correctly focus on code violations, the deeper challenge is embedding accessibility into corporate strategy and governance, not just compliance checklists.

**Wordcount:** 205

**References:**

- Cech, E.A. and Waidzunas, T.J. (2021) 'Digital Justice in Design', *Science, Technology, & Human Values*, 46(6), pp. 1201–1223.  
González, A. et al. (2023) 'Inclusive Design as a Driver of Innovation in Software Development', *Information and Software Technology*, 157, 107187.  
ISO (2019) *ISO 9241-210:2019 Ergonomics of Human-System Interaction – Human-Centred Design for Interactive Systems*. Geneva: ISO.

**Response Post 3:**

Thank your Nikolaos for your balanced Initial Post!

You offer a strong analysis of the Blocker Plus case and rightly highlight how fairness, accountability, and transparency are central to ethical AI governance. I would like to extend this position by noting that the problem goes beyond technical bias, it exposes a lack of ethical resilience in AI system design. Rahwan (2022) argues that systems should be built to anticipate adversarial manipulation and adapt to social context shifts, not just comply with static principles.

Moreover, the case reflects a persistent gap between *ethics by design* and *ethics in practice*. While guidelines like those of the EU's High-Level Expert Group on AI set high standards, developers often face institutional pressure to prioritise speed and functionality over social responsibility (Möckander and Floridi, 2023). Embedding ethical checkpoints within development pipelines could help address this.

Finally, your point about public accountability could be deepened by considering participatory AI governance, where affected communities contribute feedback on system behaviour (Whittaker et al., 2021). This would align professional ethics with democratic oversight, ensuring technology evolves in dialogue with society rather than above it.

**Wordcount:** 185

## **References:**

- Mökander, J. and Floridi, L. (2023) ‘Ethics as a Service: A Pragmatic Model for AI Governance’, *AI and Society*, 38(2), pp. 657–670.
- Rahwan, I. (2022) ‘Society-in-the-Loop: Programming the Algorithmic Social Contract’, *Ethics and Information Technology*, 24(4), pp. 1–13.
- Whittaker, M. et al. (2021) *The AI Now Report 2021: Participatory Governance in AI Systems*. New York: AI Now Institute.

## **Summary Post**

Building on the insights from Nikolaos and Tobias, it becomes evident that the *Abusive Workplace Behaviour* case exemplifies not only individual ethical failures but also systemic organisational shortcomings in fostering inclusive and psychologically safe environments. Both responses rightly highlight the collective nature of ethical responsibility; however, they underplay the significance of formal accountability mechanisms and legal compliance that I emphasised in my initial post. Ethical responsibility must operate not only at the interpersonal level but within structured frameworks of enforcement, aligning professional codes with employment law and organisational governance (Hughes, Monaghan and Allen, 2020).

While Nikolaos effectively expands on inclusiveness and diversity, his interpretation risks reducing ethical leadership to cultural values rather than binding professional obligations. The *ACM Code of Ethics* (Gotterbarn, Miller and Rogerson, 2018) and *BCS Code of Conduct* (2021) are not aspirational statements but enforceable standards that demand intervention when misconduct occurs. Without accountability, “psychological safety” risks becoming a symbolic concept rather than a professional mandate. Ethical leadership, therefore, requires according to Johnson (2020) both empathy and procedural integrity, ensuring complaints are addressed transparently and that disciplinary action reinforces ethical codes.

Tobias’s discussion of “ethical passivity” adds an important organisational lens, yet his analysis overlooks how such passivity may stem from institutional complicity, where power dynamics and reputational fears discourage reporting. As Kuteesa et al. (2024) highlight, tolerance of gender bias perpetuates systemic exclusion in technology fields, revealing that ethical cultures cannot thrive without structural reform.

Ultimately, ethical computing must integrate legal awareness, procedural safeguards, and leadership accountability to move beyond rhetoric toward tangible professional protection.

**Wordcount:** 259

## **References:**

BCS (2021) *Code of Conduct*. British Computer Society. Available at: <https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/> (Accessed: 05 November 2025).

Gotterbarn, D., Miller, K. and Rogerson, S. (2018) 'ACM Code of Ethics and Professional Conduct', *Communications of the ACM*, 61(1), pp. 21–28.

Hughes, J., Monaghan, C. and Allen, D. (2020) *Employment Law for Business Students*. 3rd edn. London: Routledge.

Johnson, D.G. (2020) *Computer Ethics*. 5th edn. Harlow: Pearson.

Kuteesa, K.N., Dagunduro, A.O., Ajuwon, O.A. and Chikwe, C.F. (2024) 'Addressing gender inequality in tech workplaces: challenges and opportunities', *Comprehensive Research and Reviews in Multidisciplinary Studies*, 2(1), pp. 19–26. Available at: <https://doi.org/10.57219/crrms.2024.2.1.0037>