Guardians' Global Code — Preamble, Articles, and Annexes (Citizens Edition)

Preamble

The Guardians' Global Code is built as both a shield and a guide. It is meant to protect humanity, the planet, and future generations from the dangers of unregulated technologies, while also providing a pathway for ethical innovation and global cooperation. The Articles that follow establish the main principles, structures, and responsibilities of governance. The Annexes then define the critical terms and technologies referenced throughout, ensuring that there is no ambiguity and that every reader — whether policymaker, scientist, advocate, or citizen — can share a common understanding.

This text is written in direct and accessible language, not as an abstract legal code but as a living framework. Its purpose is to bring clarity, strengthen accountability, and empower ordinary people to hold governments, corporations, and institutions to the highest standards. By uniting principles, policies, and definitions, the Guardians' Global Code provides a holistic system for ethical governance in the age of artificial intelligence, electronic technologies, environmental manipulation, and beyond.

Guardians' Global Code — Summary Edition (Articles I–XXXIII)

Article I — Human Supremacy Clause

This article establishes the principle that human beings must always retain ultimate authority over artificial intelligence, automated systems, and advanced technologies. It prohibits machine override in critical areas such as medicine, adjudication, weapons deployment, and democratic decision-making, requiring provable human veto paths and full audit trails for every consequential decision. The clause mandates transparent logs of all human interventions, ensuring accountability and preserving human dignity and sovereignty in the face of increasingly autonomous systems.

Article II — Fundamental Rights and Dignity

This article guarantees that all uses of AI and advanced technologies must respect the inherent rights and dignity of every individual. It prohibits discrimination, coercion, exploitation, and psychological manipulation, while requiring accessibility, disability awareness, and measurable equity outcomes. Enforceable remedies are built in: victims of AI-related harms must have access to rapid appeals, reparations funding, and pro bono counsel. The article ensures that no citizen is left without recourse when confronted with technological abuse.

Article III — Transparency, Audit, and Traceability

This article mandates a culture of radical transparency for all AI and technological deployments. It requires comprehensive documentation including model cards, data lineage maps, safety reports, red-team results, and audit packages made available to independent citizen panels. AI developers and operators must create public-grade audit trails, and overseers are granted subpoena-style powers to access safety artifacts and internal communications. This transparency obligation makes it possible for the public to verify both the design and deployment of high-risk technologies.

Article IV — Safety, Risk, and Red-Team Duty

This article creates enforceable obligations for ongoing safety testing and adversarial risk assessment across all AI and technological systems. It requires pre-deployment red-teaming, continuous stress testing, and independent third-party verification of safety claims. Organizations must document risks openly and share mitigation strategies with regulators and citizen oversight panels. Failure to conduct rigorous risk analysis is treated as a breach of duty, subject to sanctions, liability, and withdrawal of deployment authorization.

Article V — Citizen Oversight and EarthVote

This article establishes permanent citizen oversight institutions and introduces the EarthVote framework — a global, blockchain-secured voting system that enables citizens to participate directly in high-stakes governance decisions about technology. It ensures rotation of citizen panels, prevents capture by corporate or governmental elites, and guarantees that no global decision on AI, weapons, or atmospheric manipulation can proceed without transparent citizen

consultation. The EarthVote system provides legitimacy, democratization, and trust in a field often dominated by secrecy.

Article VI — Digital Immune System Clause

This article mandates the creation of a global defense system against harmful AI, cyberattacks, algorithmic manipulation, and weaponized digital signals. The “Digital Immune System” protects against invasive surveillance, hacking, data theft, and coordinated disinformation campaigns. It requires governments and corporations to contribute to shared protections, while citizen watchdogs ensure that security measures are not repurposed for oppression. The clause balances resilience with freedom by outlawing surveillance-driven “security theater” while mandating real protections against hostile intrusions.

Article VII — Fail-Safe Shutdown Protocol

This article requires that all AI and high-risk technological systems contain an enforceable, provable shutdown mechanism under human control. Such mechanisms must be tested regularly, documented, and overseen by independent citizen bodies. No technology may be deployed globally without a clear path to halting it in emergencies. The article ensures that no government, corporation, or private actor can unleash uncontrollable systems without accountability or the ability to reverse harm.

Article VIII — Data Sovereignty and Consent

This article establishes the principle that all individuals are the owners of their own data, identity, and biometrics. Collection, storage, and use of personal information must be based on informed consent, with transparent terms and options to revoke participation. Predictive analytics, biometric tracking, genome-targeting, and DNA-based surveillance are explicitly restricted. Violations of consent trigger legal penalties, reparations, and the destruction of unlawfully collected data.

Article IX — Environmental and Atmospheric Protections

This article prohibits covert or harmful manipulation of the environment through geoengineering, chemtrails, aerosol dispersals, electromagnetic emissions, or acoustic weapons. It references and strengthens the ENMOD Convention by adding enforceable penalties for atmospheric experimentation. Citizens must be informed and must consent to any environmental modification trials. The article requires independent environmental assessments, reparations for ecological damage, and international bans on using the Earth's systems as tools of warfare or control.

Article X — Prohibition of Electronic Harassment and Directed Energy Weapons

This article bans the targeting of individuals or groups with directed energy, microwave, acoustic, or frequency-based technologies. It outlaws the use of these systems for coercion, punishment, surveillance, or experimental purposes. Victims must be given immediate redress and recognition under international law, with protections similar to those against torture. Governments and militaries found complicit in such practices are subject to sanctions, international trials, and victim compensation.

Article XI — AI in Warfare and Security

This article bans autonomous lethal weapons and severely restricts the military use of AI. It requires human oversight in all battlefield decisions and prohibits experimentation on civilian populations. The article mandates international inspections of defense-related AI projects and creates citizen war-crimes review boards to ensure compliance. The principle is simple: no machine may make life-or-death decisions in warfare without human accountability.

Article XII — Economic and Financial Oversight

This article establishes global transparency requirements for financial flows related to AI, surveillance, and covert technologies. It requires disclosure of contracts, public-private partnerships, black budgets, and emergency disbursements. Financial institutions, including the IMF, World Bank, BIS, and national treasuries, must disclose AI-related funding lines. The article ensures that money trails behind covert projects are traceable, accountable, and subject to citizen review.

Article XIII — Reparations and Justice Mechanisms

This article creates enforceable obligations for reparations and compensation for victims of AI abuse, electronic harassment, and environmental manipulation. It establishes global funding pools, seeded by governments and corporations, to support victims' healthcare, legal defense, and reintegration. It also guarantees free legal counsel for those seeking justice. Reparations are treated not as charity but as a binding legal duty of those responsible for technological harm.

Article XIV — Global Legal Appeals Framework

This article establishes a universal appeals system for technology-related harms, giving citizens a fast-track path to challenge abuses. Appeals panels include both legal experts and rotating citizen members, ensuring accessibility and fairness. Cases can escalate from local to regional to global levels, with binding decisions and enforcement powers. This framework ensures that citizens have real legal recourse beyond national jurisdictions.

Article XV — Citizen Education and Literacy

This article requires all nations to implement education programs on AI, digital rights, environmental ethics, and human protections. Curricula must be accessible, multilingual, and culturally inclusive, teaching citizens how to identify and report harms. Special provisions ensure training for children, vulnerable groups, and developing nations. Education is seen as the foundation of long-term resilience against abuse.

Article XVI — Scientific and Ethical Research Standards

This article establishes global ethical standards for all scientific research involving AI, human experimentation, or environmental manipulation. It incorporates principles from the Belmont Report and Common Rule, extending them globally. Research without informed consent,

transparency, and independent ethical review is outlawed. Whistleblowers are granted protection, and violations trigger both legal liability and funding cutoffs.

Article XVII — Prohibition of Covert Infrastructure

This article bans the use of disguised infrastructure such as hidden cell towers, covert antennas, or neighborhood-based surveillance nodes. It prohibits military or corporate use of civilian buildings, hospitals, or telecom systems for covert targeting or experimentation. All infrastructure must be declared publicly and subject to inspection.

Article XVIII — Global Complaint Routing System

This article mandates the creation of a transparent, multi-tier complaint system for citizens reporting technological harms. Complaints route from local to global levels through standardized portals, with guaranteed timelines for response. Anonymous submissions are allowed, and whistleblowers are protected. Complaints must be investigated and cannot be buried or ignored.

Article XIX — No Loophole Guarantee

This article ensures that no nation, corporation, or agency can exploit legal loopholes to bypass protections. All technologies, whether named or future-developed, fall under the same protections if they harm human dignity, health, or the environment. The clause prevents evasions through classification, secrecy, or rebranding.

Article XX — Protections for Prisoners and Vulnerable Populations

This article explicitly bans experimentation on prisoners, detainees, refugees, and vulnerable communities. It requires inspections of prisons, detention centers, and refugee camps to ensure compliance. Vulnerable groups must receive special legal protections, reparations, and international oversight.

Article XXI — Corporate Accountability

This article mandates full accountability for corporations engaged in AI development, surveillance, or experimental technologies. It requires disclosure of contracts with governments, internal testing records, and whistleblower protections. Corporations are legally liable for harms caused by their technologies, with penalties including dissolution, fines, and reparations.

Article XXII — Whistleblower Protection

This article provides sweeping protections for individuals exposing covert programs, AI abuses, or environmental manipulation. Whistleblowers must be shielded from retaliation, given anonymity options, and offered reparations for personal losses. International safe havens are established for whistleblowers who flee hostile regimes.

Article XXIII — Medical Ethics and Bio-Safeguards

This article prohibits AI-driven or covert biomedical experimentation without informed consent. It outlaws genome-targeting, DNA surveillance, and hidden bio-agent dispersals. Medical programs must publish transparent protocols, with independent reviews to ensure safety. Violations are treated as crimes against humanity.

Article XXIV — Digital Identity and Autonomy

This article secures the right of citizens to control their digital identity, including accounts, communications, and online presence. It prohibits unauthorized account manipulation, shadow bans, and AI-driven reputational attacks. Citizens have the right to demand access, corrections, and restitution for compromised digital lives.

Article XXV — Independent International Scientific Panel on AI

This article establishes a permanent global scientific body, independent from corporate and state capture, to assess AI and emerging technologies. Its findings are binding inputs for governance, with the power to recommend bans, restrictions, or emergency shutdowns. Citizen members rotate on this panel to ensure balance.

Article XXVI — Amendment and Evolution Framework

This article allows the Guardians' Global Code to evolve through structured amendment processes. Amendments must pass citizen review panels and EarthVote thresholds, preventing elite capture. This ensures that the Code adapts to future technologies while preserving its protective spirit.

Article XXVII — EarthVote Voting Cycle

This article details the operational timing of global citizen votes on governance issues. Cycles are regular, accessible, multilingual, and secured by blockchain. Every citizen has equal participation rights, ensuring the democratic legitimacy of global governance decisions.

Article XXVIII — Institutional Design and Rotations

This article lays out the design of oversight institutions, including rotating citizen panels, independent courts, and global inspectorates. Rotations prevent corruption, and term limits ensure fairness. No institution may consolidate unchecked power.

Article XXIX — Reparations Fund and Compensation Channels

This article creates permanent funding channels for victims of AI, electronic harassment, and covert technologies. Funds are drawn from state contributions, corporate penalties, and international levies. Victims receive both financial restitution and access to medical, psychological, and social recovery services.

Article XXX — International Enforcement Mechanisms

This article establishes enforcement powers for the Guardians' Global Code, including international courts, sanctions, and investigative authorities. Compliance is monitored by citizen and expert teams, with binding authority to act against violators.

Article XXXI — Global Moratorium Authority

This article gives citizen panels the authority to declare moratoria on emerging technologies deemed unsafe. No new AI or experimental technology may be deployed during a moratorium period, and violators face sanctions.

Article XXXII — Global Peace and Security Integration

This article integrates the Guardians' Global Code into the UN Charter framework, ensuring peace and security considerations apply equally to technological harms. It recognizes AI and covert technologies as new threats to global peace, requiring collective security responses.

Article XXXIII — Ceremonial and Cultural Recognition

This final article establishes the Guardians' Global Code as both a legal and cultural foundation for humanity's relationship with technology. It requires ceremonial adoption,

multilingual publication, and symbolic representation (including the gold shield crest) to anchor its legitimacy in global consciousness.

Annexes I–XXXIII (Expanded Definitions)

Annex I — Artificial Intelligence (AI)

Artificial Intelligence refers to systems designed to perform tasks that normally require human intelligence, including reasoning, learning, problem-solving, and decision-making. AI includes narrow applications such as voice assistants, as well as advanced general models capable of adapting to multiple tasks.

Annex II — Machine Learning

Machine Learning is a subset of AI in which algorithms improve their performance over time by analyzing data patterns. It includes supervised learning (based on labeled data), unsupervised learning (finding hidden structures), and reinforcement learning (adapting through feedback).

Annex III — Deep Learning

Deep Learning is an advanced branch of machine learning that uses neural networks with many layers to process complex data such as images, speech, and natural language. It powers technologies like facial recognition and autonomous vehicles.

Annex IV — Algorithmic Bias

Algorithmic Bias occurs when AI systems produce unfair or discriminatory outcomes due to biased training data, flawed design, or improper oversight. It often results in inequality in hiring, policing, healthcare, or access to services.

Annex V — Data Privacy

Data Privacy refers to the right of individuals to control how their personal information is collected, stored, and used. It includes protections against unauthorized surveillance, misuse of biometric data, and intrusive digital profiling.

Annex VI — Cybersecurity

Cybersecurity is the practice of protecting digital systems, networks, and data from malicious attacks or unauthorized access. It includes encryption, secure infrastructure, and rapid response to threats.

Annex VII — Digital Identity

Digital Identity refers to the online representation of an individual, which may include names, accounts, biometric information, and behavioral data. Protecting digital identity is essential to prevent fraud, manipulation, and exploitation.

Annex VIII — Biometric Data

Biometric Data includes physical or behavioral characteristics such as fingerprints, facial scans, iris patterns, voiceprints, and gait recognition. These identifiers must remain private and under citizen control.

Annex IX — Facial Recognition

Facial Recognition is a biometric technology that identifies or verifies individuals using facial features. It raises major concerns about mass surveillance, privacy, and misuse by authoritarian regimes.

Annex X — Predictive Policing

Predictive Policing uses AI to forecast where crimes may occur or who might commit them, often reinforcing systemic bias. It is widely criticized for amplifying discrimination and eroding civil liberties.

Annex XI — Autonomous Weapons

Autonomous Weapons are systems capable of selecting and engaging targets without human intervention. They are banned under this Code due to their threat to human rights and global security.

Annex XII — Directed Energy Weapons

Directed Energy Weapons use concentrated energy, such as lasers, microwaves, or particle beams, to disable or harm targets. They can cause invisible damage to electronics, infrastructure, or people.

Annex XIII — Electromagnetic Radiation

Electromagnetic Radiation refers to waves of energy, including radio, microwaves, infrared, visible light, ultraviolet, X-rays, and gamma rays. While essential in communication and medicine, misuse can cause harm to human health and ecosystems.

Annex XIV — Microwave Weapons

Microwave Weapons emit focused microwave energy to cause pain, disorientation, or damage. Reports link them to health issues in military and diplomatic contexts, such as "Havana Syndrome."

Annex XV — Infrasound and Ultrasound

Infrasound (below human hearing) and ultrasound (above human hearing) are sound frequencies that can be used in medical imaging but also weaponized for crowd control or covert harassment.

Annex XVI — Geoengineering

Geoengineering refers to large-scale interventions in Earth's systems, such as solar radiation management or carbon capture, intended to counter climate change. Unauthorized use risks ecological imbalance and global harm.

Annex XVII — Weather Modification

Weather Modification includes techniques such as cloud seeding to alter precipitation patterns. While sometimes used for water management, it has been linked to harmful military and experimental programs.

Annex XVIII — Chemtrails (Aerosol Spraying)

Chemtrails refer to the deliberate release of aerosol substances into the atmosphere, often associated with geoengineering, climate experiments, or covert operations. These programs raise concerns about health, environment, and transparency.

Annex XIX — Nanotechnology

Nanotechnology manipulates matter at the atomic or molecular level. It offers breakthroughs in medicine and materials but also risks of misuse in surveillance, bioengineering, or weapon systems.

Annex XX — Neurotechnology

Neurotechnology interacts directly with the human brain and nervous system, including brain-computer interfaces, neural implants, and cognitive monitoring. It has potential benefits but also major privacy and ethical risks.

Annex XXI — Cognitive Warfare

Cognitive Warfare involves the manipulation of thoughts, beliefs, and perceptions using technology, propaganda, or psychological tools. It is designed to disrupt decision-making and societal trust.

Annex XXII — Human Experimentation

Human Experimentation refers to testing technologies, drugs, or methods on people, often without informed consent. History has shown the devastating harm of such practices when unchecked.

Annex XXIII — Whistleblower Protections

Whistleblower Protections safeguard individuals who reveal misconduct, corruption, or violations of this Code. These protections ensure truth-tellers are not silenced or punished.

Annex XXIV — Reparations

Reparations refer to compensation, restoration, or assistance granted to individuals or communities harmed by technologies. They ensure justice and healing for victims.

Annex XXV — Digital Immune Systems

A Digital Immune System is a defensive infrastructure designed to detect, neutralize, and respond to malicious digital threats such as cyberattacks, harmful AI, or electronic harassment.

Annex XXVI — Fail-Safe Shutdown

Fail-Safe Shutdown is the guaranteed mechanism that allows humans to deactivate an AI or technological system instantly in emergencies, ensuring safety above all else.

Annex XXVII — Citizen Oversight Panels

Citizen Oversight Panels are independent bodies of ordinary people, supported by experts, who monitor AI and technology governance, investigate complaints, and enforce accountability.

Annex XXVIII — Global Registry of AI Systems

A Global Registry of AI Systems is a publicly accessible database containing records of all high-risk AI deployments, including their purposes, risks, and oversight mechanisms.

Annex XXIX — Transparency Reports

Transparency Reports are public disclosures that provide information about how AI systems and technologies are developed, deployed, and monitored, including safety and ethics results.

Annex XXX — International Scientific Panels

International Scientific Panels are independent, rotating teams of researchers tasked with assessing the risks, impacts, and benefits of technologies in unbiased reports.

Annex XXXI — Appeals and Remedies

Appeals and Remedies provide pathways for victims or communities to challenge technological abuses and seek compensation, reparations, or justice through independent review.

Annex XXXII — Amendment Process

The Amendment Process is the structured method by which this Code can evolve, incorporating new knowledge, technologies, and citizen input while preventing corruption.

Annex XXXIII — Future Generations Clause

The Future Generations Clause ensures that decisions made today prioritize long-term well-being, sustainability, and safety for children and generations yet to be born.

The Guardians' Global Code is more than rules on paper — it is a shared promise between people everywhere. It says that technology must always serve humanity, never control or harm it. By uniting around these principles, citizens, leaders, and communities can stand together against abuse, demand accountability, and guide innovation toward what is safe, fair, and life-giving. This Code belongs to all of us, and its strength comes from the voices of ordinary people who refuse to be silent. With it, we protect not only ourselves but also our children, our planet, and the generations still to come.

May this Code stand as a shield for all people, a voice for the silenced, and a light for future generations. May it guide leaders to act with wisdom, protect the vulnerable, and heal the wounds caused by unchecked power. May every child, every community, and every nation find safety, dignity, and peace in a world where technology serves humanity. Let this work be not only a set of rules, but a living promise — that together we will guard what is sacred and build a future worthy of us all.

May God bless this Code and those who carry it forward. May He grant courage to the weary, protection to the vulnerable, and wisdom to those in power. May His light expose injustice, and His mercy bring healing where there has been harm. We ask that this work serve as a covenant of peace, justice, and truth for all nations, so that every soul may live free from fear and walk in dignity.