Title	IFIP Code of Ethics
Author(s)	Kreps, David
Publication Date	2021-08-04
Publication Information	Kreps, David. (2021). IFIP Code of Ethics. In Michael Goedicke, Erich Neuhold, & Kai Rannenberg (Eds.), Advancing Research in Information and Communication Technology: IFIP's Exciting First 60+ Years, Views from the Technical Committees and Working Groups (pp. 405-420). Cham: Springer International Publishing.
Publisher	Springer
Link to publisher's version	https://doi.org/10.1007/978-3-030-81701-5_17
Item record	http://hdl.handle.net/10379/16936
DOI	http://dx.doi.org/10.1007/978-3-030-81701-5

IFIP Code of Ethics

David Kreps[1][0000-0002-3294-0465]

[1] National University of Ireland, Galway.
[1]`david.kreps@nuigalway.ie`

Abstract. A short introduction to the creation of the IFIP Code of Ethics, followed by the Code itself.

Creating the IFIP Code of Ethics

At the virtual IFIP General Assembly (GA) held 24th September 2020, GA enthusiastically adopted a new IFIP Code of Ethics and Professional Conduct, crowning a project begun in 1988 by then TC9 Chair Harold Sackman[1]. Although countless figures in the world of ICT over the intervening decades contributed to this project, perhaps the names Jacques Berleur and Don Gotterbarn deserve special mention. Berleur and his Working Group 9.2 on Social Accountability worked tirelessly through the 1990s to push the concept of ethical computing, including the creation of IFIP Special Interest Group 9.2.2 on Framework on Ethics of Computing, and producing with members of the group the 'Criteria and Procedures for Developing Codes of Ethics or of Conduct' [1]. Gotterbarn, who had led on the 1999 joint ACM/IEEE-CS Software Engineering Code [2], also led the project to create a revised version of the ACM Code of Ethics that was published in 2018. This revised Code went through many years of consultation and development - consistent with Berleur's criteria and procedures - not just with ACM members but with members of IFIP, IEEE, other national and international bodies and companies all around the world.

Clearly a global code – the conscience of the profession – it struck David Kreps, as the current Chair of TC9, that Sackman's project could at last be completed: that IFIP could adopt this Code of Ethics and bring it to National Computing Societies the world over. Approved by the TC9 Committee meeting in Stockholm in June 2019, Gotterbarn – now Chair of WG9.2.2 – took the proposal to the Working Group who also unanimously supported it. Gotterbarn then joined Kreps, at GA 2019 in Kiev, to propose a Code of Ethics Task & Finish Group, to adapt the ACM Code, and publish it as the IFIP Code of Ethics. GA approved the proposal. Joined by IP3 Chair Moira de Roche, and MSA Representative Margaret Havey, the Code of Ethics Task & Finish Group, led by Kreps, was formally established, and undertook further consultations with Member Societies and with the IFIP Board, over the course of 2020. The group created a new Prologue contextualising the Code for the IFIP membership, producing

---

[1] See the chapter in this volume on the history of HCC and TC9 – a Sociotechnical Tale – for more detail on this decades long project.

the final version adopted at GA2020. That Prologue and the final version of the Code are presented here.

The IFIP Code of Ethics can be adopted in place of, or alongside a Member Society's Code, or Member Societies can modify their Code to include values and guidance in the IFIP Code that is not already included in their own Codes, or they can simply reference it in addition to their own codes.

In the words of Jussi Nissilä, CEO of the Finnish Information Processing Society (TIVIA) "The code has been gone through, line-by-line, by the TIVIA Working Group on Ethics, and no reason to not adopt it was found – on the contrary, the Working Group on Ethics considered it to be culture independent, and suitable for TIVIA, as well as any computing society". Maxine Leslie, Secretariat and Committee Manager at the British Computer Society, likewise, reported that "The BCS Academy of Computing has reviewed the proposed IFIP Code of Ethics and will be pleased to endorse it, finding it a very robust document covering a variety of important and interesting topics." Vicki Hanson, CEO of the ACM, said "As an international member of IFIP, ACM endorses the proposed IFIP Code of Ethics as a common international standard for computing and the profession."

It is a fitting tribute to the work of so many, that – in its 60th anniversary year – IFIP has now formally adopted this international IFIP Code of Ethics, whose creation has spanned many decades and the engagement of countless contributors from around the world.

References

1. Berleur, J., Duquenoy, P., Holvast, J., Jones, M., Kimppa, K., Sizer, R., Whitehouse, D.: Criteria and Procedures for Developing Codes of Ethics or of Conduct. On behalf of IFIP-SIG9.2.2 IFIP Press, Laxenburg-Austria (2004).
2. Gotterbarn, D., Miller, K., and Rogerson, S.: Software Engineering Code of Ethics is Approved. Communications of the ACM 42,10,102-107. DOI: 10.1145/317665.317682 (1999)

IFIP Code of Ethics

Prologue by the IFIP Task and Finish Group

Prologue

The purposes and values of a profession, including its commitment to the public good, are expressed by its code of ethics. This Code of Ethics and Professional Conduct expresses the values and reflects the ethics of IFIP's member societies and the wider profession. It is a global statement of the conscience of the ICT profession and clarifies what our profession should strive to be: it is a call to action.

Professional ethics is about what is expected of a professional in a field. As we act, all of us in the ICT Profession must remember that every choice that impacts others is an ethical decision and that those decisions need to be guided by professional ethics. The competent application of ICT technical skills is necessary for the well-being of contemporary society; our technical skills are important, but how we apply them is what distinguishes us as professionals. Professionals are asked to promote good while working within ethical constraints.

The IFIP Code of Ethics [the Code] provides organizations and governments around the world with a common set of values that should be reflected in codes of ethics for all parts of the ICT profession. The Code promotes the continued development of a global conscience within the ICT sector, providing a common ground for international discourse on professional responsibility.

Development of the Code

This Code is a response to the degree to which the work of ICT professionals in the 21st-century influences and directs all aspects of society. Our times demand a re-examination and re-statement of the professional responsibilities of ICT practitioners. A clear understanding of these ethical principles is needed to help guide ICT professional practice to positively contribute to society in ways that minimize unintentional ethical mistakes and maximize ethical opportunities.

IFIP has a long tradition of support for ethical and professional standards. One of IFIP's major responses to this need has been the development and support of the International Professional Practice Partnership (IP3), an international multi-society consortium formed to promote the professionalization of ICT. At its founding meeting in 2008 IFIP's IP3 identified Four Pillars of the ICT Profession. Pillars 1 and 2 focus on professional competence while Pillars 3 and 4 recognize the nature of ICT as employing these skills in service to society. The Four Pillars are about normative ethics - what you should do in any given circumstance. Professional ethics is about what is expected of a professional in a field. This IFIP Code of Ethics is a statement of professional ethics.

IFIP has a Technical Committee on ICT and Society and a Special Interest Group on the Ethics of Computing. The latter was charged with developing a Code of Ethics and

Professional Conduct and decided to base this closely on the Code of Ethics prepared by ACM. There are a number of reasons for adapting the ACM Code into an IFIP Code. IFIP was involved in the most recent update of the ACM Code, the objective of which was to define and articulate ICT's professional obligations to the much broader range of stakeholders impacted by modern ICT systems and the requirement for the code to address the intercultural common ethical obligations of its international membership. The development involved extensive worldwide consultation and was consistent with the 1996 IFIP SIG 9.2.2 Framework for Developing a Code of Ethics written under the guidance of the late Jacques Berleur. IFIP was well represented in the transparent multi-year iterative Code development process.

The IFIP Code of Ethics as it finally came together as presented in this publication supports the IP3 Four Pillars. With contributions by IFIP members and the international community. the Code is consistent with the diverse Codes of member societies. It is a global Code created by people from all over the world including members of IFIP.

The Nature of the Code

Older Codes of Ethics contained specific imperatives or benchmarks which could be used to determine failure to follow a particular Code canon. Codes with fixed benchmarks, however, are of little help in a rapidly changing ICT environment and do not help practitioners make proactive decisions in complex situations. Meeting these needs requires aspirational guidance that can accommodate a rapidly changing profession.

ICT professionals, regardless of where they live and work, have more in common than they think. Different nationalities have diverse cultures, but multinational organizations based on a common profession share significant values to be embodied in a Code, which should articulate the global values of the profession not the differences between cultures. Intercultural global values we have in common establish a discursive ethics on which we can all make decisions.

Those values need to be presented in a reasonably achievable fashion. Instead of fixed rules, the Code therefore is based on an aspirational model setting ethical targets rather than tying an ethical value to the use of a particular technological solution. These ethical markers of professionalism are presented as goals and ideals to which the morally responsible professional practitioner aspires. The Code provides some guidance in decision making in unclear and difficult situations, but it also respects the autonomy of the individual professional. The primary goal in the Code is consistent with the international standards in the IP3 Four Pillars: to establish the Public Good as the primary focus of our profession.

Structure of the Code

The Code consists of a Preamble that describes the Code and provides some guidance about reasoning with its Principles. The remainder of the Code consists of 25 Principles divided into four sections; each Principle is accompanied by guidance that further explains the Principles and illustrates the application of it to ICT.

The Preamble points to a maxim that should be used to frame any decision made using the Code. Consistent with the IP3 Pillars and most other Codes recognizing ICT's positive public responsibility, "the public good is the paramount consideration." The common conscience of the profession is that our work should contribute to society and human well-being, acknowledging that all people are stakeholders in computing. The Code applies that global principle.

The four sections of the remainder of the Code consist of Principles one should aspire to. Section 1 "General Ethical Principles" contains seven common ethical principles consistent with all professional codes. Section 2 "Professional Responsibilities" provides nine specific ICT professional responsibilities in the light of the general principles of section 1. Section 3 "Professional Leadership Principles" adds seven responsibilities to ICT professionals when they have leadership responsibilities. Each of these Principles is accompanied by some guidance on how that Principle might apply to professional decisions. Putting these Principles in context and relating them to a common ethical foundation helps practitioners understand how these broad Principles apply to their decisions in specific instances and how to incorporate them into their regular practice of the profession. In that way, the Code is a guide to proactive action that helps us, as a profession, to promote good.

The predominant direction of the Code provides guidance for the ICT professional. Only 2 of the 25 Principles deal with compliance. Given the proactive nature of the Code, the compliance section advocates active support for the Code Principles beyond mere compliance. That support includes both a professional's advocacy for the principles and working to correct situations where the principles are not being followed.

Status

In joining a Technical Committee, Working Group, Special Interest Group, Domain Committee, IP3, or other body or structure of IFIP, members agree to adhere to and support this Code of Ethics.

The IFIP Code of Ethics is compulsory for all serving on the General Assembly or ex-officio members of IFIP.

The IFIP Code of Ethics is not intended to replace Codes specific to Member Societies, which may contain unique points relevant to their cultures. The Code contains elements, however, that might not be included in the Member Society Code. Therefore, the IFIP Code of Ethics can be adopted alongside a Member Society's Code, or Member Societies can modify their Code to include those values and guidance not already included in their own Codes or simply reference it in addition to their own codes.

In this way, when a member of one National Computing Society works in another country, there is a common standard they can appeal to when pursuing development as an ethical professional, making ethically sound decisions when given the opportunity, and when resisting unethical pressures. The Code thereby represents a support for moral courage, encompassing the duty of care and accountability to minimize any adverse impacts as technologies are being integrated into virtually every sector of the economy and society.

Benefits of the Code

- is consistent with and extends the impact of IP3's Four Pillars
- provides a consistent international statement of ICT values
- is an argument against those who say there are no real ICT standards, but only multiple local policies
- educates the public
- is useful international statement of values.in cross-border judicial discussions
- expresses the intercultural aspects of global ICT
- is a common ground for international discourse on professional responsibility
- adequately reflects the ethics of the profession, and clarifies what that profession should strive to be
- can be used to educate aspiring ICT professionals about their ethical obligations
- can be used to evaluate the consistency of a professional's behavior with the conscience of the profession and the application of appropriate sanctions

Summary

The Code establishes goals that are valued by the ICT professional to help professionals around the world, describing what brings us together as a profession. It expresses a social contract we have as a professional society, as members of IFIP, a contract describing what we expect of each other and ourselves as members of IFIP. It provides guidance to IFIP members about committing to ethical professional conduct. The Code identifies fundamental considerations for contributing to societal aspirations and human well-being.

IFIP Code of Ethics and Professional Conduct

Preamble

Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good. This code is adapted from the ACM Code of Ethics and Professional Conduct ("The Code"), which expresses the conscience of the profession.

The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. Additionally, the Code serves as a basis for remediation when violations occur. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration. Each principle is supplemented by guidelines, which provide explanations to assist computing professionals in understanding and applying the principle.

Section 1 outlines fundamental ethical principles that form the basis for the remainder of the Code. Section 2 addresses additional, more specific considerations of professional responsibility. Section 3 guides individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every IFIP member, and principles involving compliance with the Code are given in Section 4.

The Code as a whole is concerned with how fundamental ethical principles apply to a computing professional's conduct. The Code is not an algorithm for solving ethical problems; rather it serves as a basis for ethical decision-making. When thinking through a particular issue, a computing professional may find that multiple principles should be taken into account, and that different principles will have different relevance to the issue. Questions related to these kinds of issues can best be answered by thoughtful consideration of the fundamental ethical principles, understanding that the public good is the paramount consideration. The entire computing profession benefits when the ethical decision-making process is accountable to and transparent to all stakeholders. Open discussions about ethical issues promote this accountability and transparency.

1   GENERAL ETHICAL PRINCIPLES.

A computing professional should...

1.1   Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to

autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority.

Computing professionals should consider whether the results of their efforts will respect diversity, will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work that benefits the public good.

In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals should promote environmental sustainability both locally and globally.

1.2   Avoid harm.

In this document, "harm" means negative consequences, especially when those consequences are significant and unjust. Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive.

Well-intended actions, including those that accomplish assigned duties, may lead to harm. When that harm is unintended, those responsible are obliged to undo or mitigate the harm as much as possible. Avoiding harm begins with careful consideration of potential impacts on all those affected by decisions. When harm is an intentional part of the system, those responsible are obligated to ensure that the harm is ethically justified and to minimize unintended harm.

To minimize the possibility of indirectly or unintentionally harming others, computing professionals should follow generally accepted best practices unless there is a compelling ethical reason to do otherwise. Additionally, the consequences of data aggregation and emergent properties of systems should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.

A computing professional has an additional obligation to report any signs of system risks that might result in harm. If leaders do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, a computing professional should carefully assess relevant aspects of the situation.

1.3   Be honest and trustworthy.

Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.

Computing professionals should be honest about their qualifications, and about any limitations in their competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to either real or perceived conflicts

of interest or otherwise tend to undermine the independence of their judgment. Furthermore, commitments should be honored.

Computing professionals should not misrepresent an organization's policies or procedures, and should not speak on behalf of an organization unless authorized to do so.

1.4   Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and justice govern this principle. Fairness requires that even careful decision processes provide some avenue for redress of grievances.

Computing professionals should foster fair participation of all people, including those of underrepresented groups. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, nationality, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of the Code. Harassment, including sexual harassment, bullying, and other abuses of power and authority, is a form of discrimination that, amongst other harms, limits fair access to the virtual and physical spaces where such harassment takes place.

The use of information and technology may cause new, or enhance existing, inequities. Technologies and practices should be as inclusive and accessible as possible and computing professionals should take action to avoid creating systems or technologies that disenfranchise or oppress people. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.

1.5   Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

Developing new ideas, inventions, creative works, and computing artifacts creates value for society, and those who expend this effort should expect to gain value from their work. Computing professionals should therefore credit the creators of ideas, inventions, work, and artifacts, and respect copyrights, patents, trade secrets, license agreements, and other methods of protecting authors' works.

Both custom and the law recognize that some exceptions to a creator's control of a work are necessary for the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works. Efforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and work put into the public domain. Computing professionals should not claim private ownership of work that they or others have shared as public resources.

1.6   Respect privacy.

The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the

people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.

Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections.

1.7   Honor confidentiality.

Computing professionals are often entrusted with confidential information such as trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly articles, and patent applications. Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities. A computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

2   PROFESSIONAL RESPONSIBILITIES.

A computing professional should...

2.1   Strive to achieve high quality in both the processes and products of professional work.

Computing professionals should insist on and support high quality work from themselves and from colleagues. The dignity of employers, employees, colleagues, clients, users, and anyone else affected either directly or indirectly by the work should be respected throughout the process. Computing professionals should respect the right of those involved to transparent communication about the project. Professionals should be

cognizant of any serious negative consequences affecting any stakeholder that may result from poor quality work and should resist inducements to neglect this responsibility.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

High quality computing depends on individuals and teams who take personal and group responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and with awareness of the social context in which their work may be deployed. Professional competence also requires skill in communication, in reflective analysis, and in recognizing and navigating ethical challenges. Upgrading skills should be an ongoing process and might include independent study, attending conferences or seminars, and other informal or formal education. Professional organizations and employers should encourage and facilitate these activities.

2.3 Know and respect existing rules pertaining to professional work.

"Rules" here include local, regional, national, and international laws and regulations, as well as any policies and procedures of the organizations to which the professional belongs. Computing professionals must abide by these rules unless there is a compelling ethical justification to do otherwise. Rules that are judged unethical should be challenged. A rule may be unethical when it has an inadequate moral basis or causes recognizable harm. A computing professional should consider challenging the rule through existing channels before violating the rule. A computing professional who decides to violate a rule because it is unethical, or for any other reason, must consider potential consequences and accept responsibility for that action.

2.4 Accept and provide appropriate professional review.

High quality professional work in computing depends on professional review at all stages. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical reviews of others' work.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computing professionals are in a position of trust, and therefore have a special responsibility to provide objective, credible evaluations and testimony to employers, employees, clients, users, and the public. Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Extraordinary care should be taken to identify and mitigate potential risks in machine learning systems. A system for which future risks cannot be reliably predicted requires frequent reassessment of risk as the system evolves in

use, or it should not be deployed. Any issues that might result in major risk must be reported to appropriate parties.

2.6   Perform work only in areas of competence.

A computing professional is responsible for evaluating potential work assignments. This includes evaluating the work's feasibility and advisability, and making a judgment about whether the work assignment is within the professional's areas of competence. If at any time before or during the work assignment the professional identifies a lack of a necessary expertise, they must disclose this to the employer or client. The client or employer may decide to pursue the assignment with the professional after additional time to acquire the necessary competencies, to pursue the assignment with someone else who has the required expertise, or to forgo the assignment. A computing professional's ethical judgment should be the final guide in deciding whether to work on the assignment.

2.7   Foster public awareness and understanding of computing, related technologies, and their consequences.

As appropriate to the context and one's abilities, computing professionals should share technical knowledge with the public, foster awareness of computing, and encourage understanding of computing. These communications with the public should be clear, respectful, and welcoming. Important issues include the impacts of computer systems, their limitations, their vulnerabilities, and the opportunities that they present. Additionally, a computing professional should respectfully address inaccurate or misleading information related to computing.

2.8   Access computing and communication resources only when authorized or when compelled by the public good.

Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code. Consequently, computing professionals should not access another's computer system, software, or data without a reasonable belief that such an action would be authorized or a compelling belief that it is consistent with the public good. A system being publicly accessible is not sufficient grounds on its own to imply authorization. Under exceptional circumstances a computing professional may use unauthorized access to disrupt or inhibit the functioning of malicious systems; extraordinary precautions must be taken in these instances to avoid harm to others.

2.9   Design and implement systems that are robustly and usably secure.

Breaches of computer security cause harm. Robust security should be a primary consideration when designing and implementing systems. Computing professionals should

perform due diligence to ensure the system functions as intended, and take appropriate action to secure resources against accidental and intentional misuse, modification, and denial of service. As threats can arise and change after a system is deployed, computing professionals should integrate mitigation techniques and policies, such as monitoring, patching, and vulnerability reporting. Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner, providing appropriate guidance and remediation.

To ensure the system achieves its intended purpose, security features should be designed to be as intuitive and easy to use as possible. Computing professionals should discourage security precautions that are too confusing, are situationally inappropriate, or otherwise inhibit legitimate use.

In cases where misuse or harm are predictable or unavoidable, the best option may be to not implement the system.

3 PROFESSIONAL LEADERSHIP PRINCIPLES.

Leadership may either be a formal designation or arise informally from influence over others. In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. While these principles apply to all computing professionals, leaders bear a heightened responsibility to uphold and promote them, both within and through their organizations.

A computing professional, especially one acting as a leader, should...

3.1 Ensure that the public good is the central concern during all professional computing work.

People—including users, customers, colleagues, and others affected directly or indirectly—should always be the central concern in computing. The public good should always be an explicit consideration when evaluating tasks associated with research, requirements analysis, design, implementation, testing, validation, deployment, maintenance, retirement, and disposal. Computing professionals should keep this focus no matter which methodologies or techniques they use in their practice.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.

Technical organizations and groups affect broader society, and their leaders should accept the associated responsibilities. Organizations—through procedures and attitudes oriented toward quality, transparency, and the welfare of society—reduce harm to the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation of computing professionals in meeting relevant social responsibilities and discourage tendencies to do otherwise.

14

3.3 Manage personnel and resources to enhance the quality of working life.

Leaders should ensure that they enhance, not degrade, the quality of working life. Leaders should consider the personal and professional development, accessibility requirements, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be used in the workplace.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.

Leaders should pursue clearly defined organizational policies that are consistent with the Code and effectively communicate them to relevant stakeholders. In addition, leaders should encourage and reward compliance with those policies, and take appropriate action when policies are violated. Designing or implementing processes that deliberately or negligently violate, or tend to enable the violation of, the Code's principles is ethically unacceptable.

3.5 Create opportunities for members of the organization or group to grow as professionals.

Educational opportunities are essential for all organization and group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties. These opportunities should include experiences that familiarize computing professionals with the consequences and limitations of particular types of systems. Computing professionals should be fully aware of the dangers of oversimplified approaches, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and their contexts, and other issues related to the complexity of their profession—and thus be confident in taking on responsibilities for the work that they do.

3.6 Use care when modifying or retiring systems.

Interface changes, the removal of features, and even software updates have an impact on the productivity of users and the quality of their work. Leaders should take care when changing or discontinuing support for system features on which people still depend. Leaders should thoroughly investigate viable alternatives to removing support for a legacy system. If these alternatives are unacceptably risky or impractical, the developer should assist stakeholders' graceful migration from the system to an alternative. Users should be notified of the risks of continued use of the unsupported system long before support ends. Computing professionals should assist system users in monitoring the operational viability of their computing systems, and help them understand that timely replacement of inappropriate or outdated features or entire systems may be needed.

3.7   Recognize and take special care of systems that become integrated into the infrastructure of society.

Even the simplest computer systems have the potential to impact all aspects of society when integrated with everyday activities such as commerce, travel, government, healthcare, and education. When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems. Part of that stewardship requires establishing policies for fair system access, including for those who may have been excluded. That stewardship also requires that computing professionals monitor the level of integration of their systems into the infrastructure of society. As the level of adoption changes, the ethical responsibilities of the organization or group are likely to change as well. Continual monitoring of how society is using a system will allow the organization or group to remain consistent with their ethical obligations outlined in the Code. When appropriate standards of care do not exist, computing professionals have a duty to ensure they are developed.

4   COMPLIANCE WITH THE CODE.

A computing professional should...

4.1   Uphold, promote, and respect the principles of the Code.

The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles of the Code and contribute to improving them. Computing professionals who recognize breaches of the Code should take actions to resolve the ethical issues they recognize, including, when reasonable, expressing their concern to the person or persons thought to be violating the Code.

4.2   Treat violations of the Code as inconsistent with the values of IFIP and its member societies.

Each IFIP member society should encourage and support adherence by all computing professionals regardless of IFIP membership. Individuals in IFIP member societies who recognize a breach of the Code should report the violation to their society, which may result in remedial action as specified in the individual member society's Code of Ethics and Professional Conduct Enforcement Policy.

The Code and guidelines were developed by the ACM Code 2018 Task Force: Executive Committee Don Gotterbarn* (Chair), Bo Brinkman, Catherine Flick*, Michael S Kirkpatrick, Keith Miller, Kate Varansky, and Marty J Wolf. Members: Eve Anderson, Ron Anderson, Amy Bruckman, Karla Carter, Michael Davis, Penny Duquenoy*, Jeremy Epstein, Kai Kimppa*, Lorraine Kisselburgh, Shrawan Kumar, Andrew McGettrick, Natasa Milic-Frayling, Denise Oram*, Simon Rogerson, David Shama, Janice Sipior, Eugene Spafford, and Les Waguespack. The Task Force was organized by the ACM Committee on Professional Ethics. Significant contributions to the Code were also made by the broader international ACM membership, including many IFIP members (marked with *).

This Code may be published without permission as long as it is not changed in any way and it carries the copyright notice.

Copyright (c) 2018 by the Association for Computing Machinery.

CONTRIBUTORS

Principle 2.5 stipulates that we should give proper credit to the creators of ideas. In some cases, such as the creation of this Code, that is a difficult task. The Code lists a range of people on organized committees who contributed to the Code, but this does not tell the full story of the many people around the world who thought ethics important enough to take their time and make positive contributions and corrections in the creation of this Code. A brilliant Australian on the executive committee drafted the intellectual property Principle. An anonymous commentator from a company in Italy was the impetus for Principle 2.9 addressing how failure to update systems facilitates the development of ransomware. This contributor was a member of one of the many groups commenting on the Code. The revision and the guidance of the "Harm clause" benefited from an extensive and heartfelt discussion on Twitter, Reddit, and other platforms with some discussants using pseudonyms. Anonymous contribution enables free and open comments but, inevitably, limits giving adequate credit for significant contributions and the countries they were from.

There were a number of task forces organized to respond to each draft, with members from industry and professional societies, some of whom represented subgroups they had organized to comment on the Code drafts rather than their company, country, or professional society; several IFIP members were involved in each of these groups. Taskforce affiliations also included ACM China, Europe, and India; ACM-W; Centre for Computing and Social Responsibility; Center for the Study of Ethics in the Profes-

sions; Deutsche Gesellschaft für Informatik; IEEE certification and Professional education; Google; Hoffman Business Ethics Center-Bentley; IFIP TC 9; IFIP WG 9.2; IFIP SIG 9.2.2 Ethical Frameworks; Intel; Microsoft Research; Oracle; Politecnico di Torino; Research Center on Computing and Society; Tata Consultancy Services; Tata Research and Design; and the US Technology Policy Committee.

These contributors represented an international collection of Computer Science, Information Systems, and Software Engineering departments and independent professionals in information systems management and development. Taskforce members were from Australia, Belgium, Canada, China, Denmark, England, Finland, Germany, Greece, India, Italy, Japan, Malaysia, Netherlands, New Zealand, Sweden, and the United States.

IFIP Task and Finish Group

Constituted at the IFIP General Assembly in Kiev in September 2019, the Task and Finish Group composed and prepared this document between October 2019 and August 2020. It was ratified and adopted at the IFIP General Assembly in September 2020.

Chair: David Kreps. David Kreps is a Philosopher of Information Systems at the National University of Ireland, Galway. He is Chair of IFIP Technical Committee 9 on ICTs and Society and a member of the IFIP Board. David is author of a range of books and papers on the philosophical and ethical aspects of the development of information systems and contemporary digital transformation.

Moira de Roche. Moira de Roche is an independent consultant. She is the Chair of IFIP International Professional Practice Partnership (IP3), and a member of the IFIP board. Moira is a Professional Member and Fellow of IITPSA. She is also a member of ACM. She is convinced that every decision must be viewed through an ethical lens.

Don Gotterbarn. Don Gotterbarn, an evangelist for professional computing, has extensive experience in academe and software systems development. He has spent several decades promoting responsible computing practices including leading the 2018 update of the ACM Code of Ethics and the development of the IEEE/ACM Software Engineering Code of Ethics and Professional Practice.

Margaret Havey. Margaret Havey is a Technical Advisor with Shared Services Canada, the Department responsible for the Government of Canada's ICT Infrastructures. She is a Professional Member and Fellow of CIPS, and is the Canada Country Member Representative to IFIP. Margaret became involved in ICT ethics in the early 2000's drafting a major revision to the CIPS Code of Ethics. She has a special interest in practical ethics.