DOI:10.1145/3173016

Don Gotterbarn, Amy Bruckman, Catherine Flick, Keith Miller, and Marty J. Wolf

ACM Code of Ethics: A Guide for Positive Action

THE ACM CODE of Ethics and Professional Conduct (the Code) is being updated by the Code Update Task Force[a] in conjunction with the ACM's Committee on Professional Ethics. The Code was initially written in 1992, and this is the first update since then. In previous articles we detailed the motivations for updating the Code,[b] gave our responses to feedback on the initial draft, and produced an updated version, which we presented for feedback through the ACM Discourse site, email, and focus groups and workshops at ETHICOMP and SIGCSE. We thank everyone who took part in this public consultation round. Their insights, both positive and negative, were invaluable. We have deliberated extensively on the numerous suggestions for additions, changes, and deletions. Based on those deliberations, we produced Draft 3 of the Code.

There are some significant changes made in Draft 3. Some principles have been removed entirely or completely rewritten, and some new principles were added in response to recommendations by several respondents. This article explains the significant changes that were made, and a few changes that were suggested but not made. For the most part, the suggestions that were not explicitly incorporated are ideas that we consider covered by existing aspects of the Code. Some of these suggestions were excellent, and because of them, explanatory materials that will supplement the Code are being designed. These include examples, cases, and more detailed explanations of the Code.

This article is part of the final round of public consultation associated with the 2018 update to the ACM Code of Ethics. ACM members agree to abide by the Code. Please encourage other computing professionals around you to read and contribute to this effort.

We have provided two opportunities to comment on this draft and suggest ways it might be improved. We have provided a space for open discussion of Draft 3 among interested parties at the ACM Code 2018 Discussion website https://code2018.acm.org/discuss. In addition, ACM members are encouraged to take an online survey about the specific principles of the Code at https://www.acm.org/code-2018-survey. Both comment systems close **Feb. 10, 2018**.

The ACM is a professional society whose goals include promotion of the highest standards "to advance the profession and make a positive impact." Thus, the ACM Code of Ethics and Professional Conduct ought to reflect the conscience of the computing profession, understood in the broadest sense. A successful code of ethics should reflect the values of the computing profession in a way that can help ACM members make appropriate ethical decisions. The Code should also inspire members, future members, and other professionals by highlighting the aspirations of the profession.

The ACM Code of Ethics and Professional Conduct is a guide to proactive action that helps us, as a profession, promote good. Because of this, it also applies to those aspiring to be computing professionals, including students. Members of ACM student chapters are also invited to take the survey and comment on the Code.

In the Code we identify global ethical principles that reflect the highest standards of computing professionals. The Code is designed to inform ACM members and others of what society should expect from computing professionals, and what computer professionals should expect of themselves.

In the next section we identify specific changes we made in response to suggestions from the reviewers. The section after that addresses some of the thoughtful suggestions that did not directly lead to changes. The article concludes with Draft 3 of the Code for your review.[c]

I. Changes from Draft 2 to Draft 3

1.2 Harm

There were several comments about Principle 1.2: Avoid Harm. Some respondents suggested that this principle was inconsistent with work in the military sector or law enforcement where some systems are designed, in part, to cause harm. The Task Force modified the guidance for this Principle to deal more effectively with that perception. Another concern expressed was that with most systems harm of some degree almost always happens. In response, we sharpened the definitions of intentional and unintentional harms, and we added language to encourage professionals to take care to minimize unintended harm.

1.3 Transparency and Honesty

Commenters were concerned that certain technological developments such as algorithmic transparency and systems that learn were not addressed by the Code. We agreed. However, since one goal of this update process is to craft language that will apply to new technologies as they emerge, we did not include these specific technologies explicitly in the Code. Instead, we tried to use language that would implicitly include them and future developments. Certain aspects of algorithmic transparency are covered by the principles regarding nondiscrimination and privacy, but the concept of transparency was not addressed in Draft 2, except with respect to the actions of people. By changing the guidance for Principle 1.3 on honesty to include explicit discussion of transparency, especially with respect to system limitations

[a] For a list of current taskforce members see http://ethics.acm.org/code-2018.

[b] http://cacm.acm.org/magazines/2016/12/210366-the-acm-code-of-ethics/fulltext

[c] A complete track changes version of Draft 3 showing additions and deletions to draft 2 is available at http://ethics.acm.org/code-2018.

and problems, the Code now addresses technologies that are opaque even to their developers. Suggestions about how to manage the release of self-modifying systems are also now made in the guidance for Principle 2.5.

> **A successful code of ethics should reflect the values of the computing profession in a way that can help ACM members make appropriate ethical decisions.**

1.4 Harassment

The harassment principle generated much discussion, both for and against a new emphasis in Draft 2 on discouraging harassment. The Task Force consensus is that a strong clause about harassment should be included in the Code since it is to be a modern statement of the ethical responsibilities of the computing profession. As an update to the previous draft, we added virtual spaces to physical spaces as places where harassment can take place. We also broadened the harassment definition to encompass cyber bullying.

Many existing harassment policies focus exclusively on prohibiting negative actions. Draft 3 of the Code now includes a proactive call to create open and inclusive spaces. We wanted to clarify that when people feel disrespected, this can also be prohibitive to certain spaces. The new language explicitly encourages building diversity and safe environments that enable all people to feel respected.

1.6 Data collection and informed consent

In Principle 1.6, Respect Privacy, we have shifted the focus away from opting in or out of data collection, and moved to a more general requirement for informed consent procedures. The stronger emphasis on informed consent requires that users not only understand what data are being collected and what they are being used for, but that they have the ability to consent to, or to withhold consent from the data collection. This is consistent with broader international standards that are being implemented worldwide, such as the European Union's General Data Protection Regulation (GDPR),[d] which we endorse.

It is important for professionals to understand that informed consent is not just about disclosure of information about data collection (for example, in a lengthy, practically unintelligible Privacy Policy), but is ideally a proactive agreement with the user about the type, content, and use of data that are being collected about them. Users should have the ability to view and update their data, and to withdraw from data collection procedures. In many circumstances, users should also be able to remove their data entirely, particularly on social media or other user-generated content platforms.

Legislation is constantly changing to catch up with technology, and different countries have different ways of approaching the issues raised by technical developments. One suggestion that was made was that we include the "right to be forgotten" in our privacy clause. This issue is a significant aspect of the EU's GDPR regulation that is coming into effect in 2018, and which has been debated in other jurisdictions as well. While we are generally supportive of this idea, we felt that for a code of ethics, the use of this term was too specific to particular legislation, and would require too nuanced a definition to be useful in this Code. Instead, as part of the privacy clause, we have required computing professionals to allow for the user's removal of data where appropriate - this captures the essence of the "right to be forgotten" in a way that we deemed to be more generalizable.

2.6 Evaluation of work and skills

Principle 2.6 clarifies the computing professional's responsibility to evaluate potential work assignments. When potential tasks are assigned, the professional should be able to evaluate the advisability and feasibility of the assignment; if these evaluations are beyond the computing professional's skill, then he or she ought to seek help in these evaluations. Professionals should further evaluate if their skill level is currently adequate to complete the assignment or if they are capable of gaining the required skills.

New Principles and Concepts

To address some of the more recent changes in computing and society we added some new principles. These principles bring attention to the professional's responsibility to a broader range of stakeholders.

[d] http://www.eugdpr.org/

2.9 Security

Computing professionals have a responsibility to ensure that the systems they create are secure. Principle 2.9 is new, and instructs professionals to "Design and implement systems that are robustly and usably secure." Computer hacking is a growing problem, and developments like ubiquitous computing and the "Internet of things" surround us with new vulnerabilities. True security requires usability—security features are of no practical use if users cannot or will not use them.

3.6 Legacy Systems Retirement

Principle 3.6 is new, and includes: "Retire legacy systems with care." This principle was added to address a fundamental tension mentioned by responders: sometimes software companies must end support for systems; however, what should they do if there are users who still depend on those systems? Discontinuing support causes harm, but sometimes is necessary. This is particularly challenging because the users of legacy systems often reside in the developing world or in areas that are economically less advantaged. This new principle says that this process should be undertaken with care, and states that it is critical to notify users of the risks (especially with regard to security) of continuing to use unsupported systems.

3.4 Leadership principle changes

In the new draft version of Principle 3.4, we consolidated Principles 3.4 and 3.5 from the previous draft. Based on respondents' comments, the Task Force decided that policies for the use of organizational computing resources are no longer such a central a concern so as to require an entire principle to itself. Instead, we amended the original principle 3.5, which was about creating policies that protect dignity, to be broader. Leaders are now expected to create and support policies and processes that not only protect dignity, but that reflect all the principles in the Code. This subsumed the original 3.4 principle, so 3.4 was eliminated, and the remaining principles were renumbered appropriately.

4 Compliance

The primary functions of a code of ethics are to state a profession's values and to present professionals' commitment to those values; but many codes also allude to consequences when professionals do not comply with the code. The principles in the ACM Code provide numerous behavioral targets. The 1992 Code had a single consequence for missing any of these behavioral targets: expulsion from the ACM. The compliance section of the updated ACM Code is designed to be more flexible, to inspire and educate, as well as punish when appropriate. The new version recognizes degrees of violation, and includes opportunities of remediation less severe than expulsion.

Must or Should?

Some commenters expressed concern about the use of "must" and "should" in the Code. In Draft 3, the word "must" appears three times, and the word "should" appears 76. The impetus to use "should" stems from the aspirational nature of the Code. This is the same motivation for replacing "moral imperative" with "ethical imperative" in the development of Draft 2. The use of the word "should" is also important because during ethical deliberations, the principles in the Code can come into conflict. When this occurs, thoughtful ethical analysis may require one of the principles to yield to others. If a computing professional "must" adhere to two principles and the particular situation does not allow adhering to both simultaneously, the person necessarily violates the Code, even when a course of action is ethically justified. By using "should" professionals are given the opportunity to articulate their analysis and be transparent about their ethical reasoning.

What about those three uses of "must"? The first is in the Preamble where it says "computing professionals must always support the public good." This reminds us that the public good is our paramount concern and is given more weight when principles in the Code conflict. The other two uses of "must" appear in the guidance for Principle 2.3, which speaks to following rules and laws. The guidance is clear: computing professionals must obey rules. The guidance articulates that it is possible for rules or laws to be unethical and when that is the case, they ought to be challenged. Further, the computing professionals "must" accept responsibility for their actions when they challenge rules.

II. Requested changes not specifically included

Many useful ideas were suggested that were not specifically included in the newest version of the Code. Perhaps most significantly is that some respondents thought that the Code's references to "the good of society" or "the public good" are so vague as to be meaningless. Suggestions were made to amend the Code to reflect the reality that there are many different societies, with important differences between them.

The Task Force agrees that "society" and "public" are indeed very broad, and that this breadth can be a symptom of insensitivity to the nuances of different groups and people. However, in writing a code of ethics for a global audience, authors can use a broad generalized term, focus on a single or a few particular societies, try to make a comprehensive list of relevant societies, or abandon any mention of "society." The Task Force decided that for practical reasons, the broad general references were the proper choice for this code. Thus, in the Code the "public" or "society" is meant to encompass all affected people, and is not meant to homogenize their diversities. In the Code, a term such as "the public good" implicitly acknowledges that individuals and subsets within the public may differ about what is good in a particular situation, but we contend that there is a notion of "good" that resonates with people. This broad sense of good can be embraced, and a broad sense of evil can be shunned, without denying the importance of diversity.

Additionally, a complete cyber security standard and a complete due process standard for Code violators were suggested to be a part of the updated Code, but were not added. Although these suggested additions reflect important concerns, the Task Force decided that the additions would be more appropriately placed in different documents. For example, they could be added as independent standards supporting the Code, such as ACM Bylaws; and they could be added in supplemental materials, such as teaching materials. There are many items that are important, even crucial, that are nonetheless not appropriate in the Code.

It is important, and tricky, to get the length of the Code right. There were some calls for the Code to be made shorter, possibly short enough to fit on a business card. There are legitimate concerns about someone choosing not to read the Code because it is too long. Rather than opt for that kind of brevity, we have targeted a middle ground. The Code must reflect the diversity of the activities computing professionals are involved in. Broader impacts of technology are not always clear or immediate, and the Code contains language to remind the reader to consider those broader impacts. Furthermore, the Code is intended to serve as a tool to use during ethical analysis. The guidance helps the professional to a deeper understanding of the principles. We hope that the Code is written in a way that facilitates a quick scan, as well as rewarding a more careful reading.

Call to action

After reading Draft 3 of the ACM Code of Ethics, please take the opportunity to make it better as a standard for the computing profession. We have provided two opportunities for you to share your comments. There is a general discussion board https://code2018.acm.org/discuss providing an opportunity for interested parties to discuss the suggested updates and ACM members are invited to take an online survey about the specific elements of the Code at https://www.acm.org/code-2018-survey. Both comment systems close **Feb. 10, 2018.**

We look forward to your comments.

III. ACM Code of Ethics and Professional Conduct: Draft 3

Draft 3 was developed by The Code 2018 Task Force. (It is based on the 2018 ACM Code of Ethics and Professional Conduct: Draft 2).

Preamble

The actions of computing professionals directly impact significant aspects of society. In order to meet their responsibilities, computing professionals must always support the public good. The ACM Code of Ethics and Professional Conduct ("the Code") reflects this obligation by expressing the conscience of the profession and provides guidance to support ethical conduct of all computing professionals.

The Code is designed to support all computing professionals, including current and aspiring computing practitioners, instructors, influencers, and anyone who uses 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 pertains to individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM 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 promotes this accountability and transparency.

1. GENERAL MORAL 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, concerning the quality of life of all people, affirms an obligation of computing professionals 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 in day-to-day decisions. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy.

Computing professionals should consider whether the results of their efforts 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. When the interests of multiple groups conflict, the needs of the least advantaged should be given increased attention and priority.

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 to any stakeholder, 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 obligated 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 tential 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 harming others, computing professionals should follow generally accepted best practices. Additionally, the consequences of emergent systems and data aggregation 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 thoroughly assess all relevant aspects.

1.3 Be honest and trustworthy.
Honesty is an essential component of trust. A computing professional should be transparent and provide full disclosure of all pertinent system limitations and potential problems. Making deliberately false or misleading claims, fabricating or falsifying data, and other dishonest conduct are violations of the Code.

Computing professionals should be honest about their qualifications, and about any limitations in competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to conflicts of interest or otherwise tend to undermine the independence of their judgment.

Computing professionals often belong to organizations associated with their work. They should not misrepresent any 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. Computing professionals should strive to build diverse teams and create safe, inclusive spaces for all people, including those of underrepresented backgrounds. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, national origin, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of the Code. Harassment, including sexual harassment, is a form of discrimination that limits fair access to the virtual and physical spaces where such harassment takes place.

Inequities between individuals or different groups of people may result from the use or misuse of information and technology. Technologies and practices should be as inclusive and accessible as possible. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.

The Code is designed to support all computing professionals, including current and aspiring practitioners, instructors, influencers, and anyone who uses technology in an impactful way.

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 provide appropriate credit to the creators of ideas or work. This may be in the form of respecting authorship, copyrights, patents, trade secrets, license agreements, or other methods of assigning credit where it is due.

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 other work put into the public domain. Some work contributes to or comprises shared community resources. Computing professionals should avoid misappropriation of these resources.

1.6 Respect privacy.
The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Therefore, a computing professional should be-

come conversant in privacy's various definitions and forms.

Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Computing professionals should only use personal data for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent unauthorized data collection, ensuring the accuracy of data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to give informed consent to automatic data collection, review their personal data, correct inaccuracies, and, where appropriate, remove 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. Computing professionals should take special care for privacy when data collections are merged. Individuals or groups may be readily identifiable when several data collections are merged, even though those individuals or groups are not identifiable in any one of those collections in isolation.

1.7 Honor confidentiality.
Computing professionals should protect confidentiality unless required to do otherwise by a bona fide requirement of law or by another principle of the Code.

User data observed during the normal duties of system operation and maintenance should be treated with strict 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, and a computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

The responsibility of respecting privacy applies to computing professionals in a particularly profound way.

2. PROFESSIONAL RESPONSIBILITIES.

A computing professional should…

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

Computing professionals should insist on high quality work from themselves and from colleagues. This includes respecting the dignity of employers, colleagues, clients, users, and anyone else affected either directly or indirectly by the work. Computing professionals have an obligation to keep the client or employer properly informed about progress toward completing the work. Professionals should be cognizant of the serious negative consequences affecting any stakeholder that may result from poor quality work and should resist any 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 the work may be deployed. Professional competence also requires skill in reflective analysis and in recognizing and navigating ethical challenges. Upgrading necessary skills should be ongoing and should include independent study, conferences, seminars, and other informal or formal education. Professional organizations and employers should encourage and facilitate those activities.

2.3 Know, respect, and apply existing rules pertaining to professional work.
"Rules" here includes 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 obey 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, it is superseded by another rule, or it

causes recognizable harm that could be mitigated through its violation. 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 other's work.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computing professionals are in a position of trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. Extraordinary care should be taken to identify and mitigate potential risks in self-changing 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 should be reported.

2.6 Have the necessary expertise, or the ability to obtain that expertise, for completing a work assignment before accepting it. Once accepted, that commitment should be honored.
A computing professional is accountable for evaluating potential work assignments.

Once it is decided that a project is feasible and advisable, the professional should make a judgment about whether the work assignment is appropriate to the professional's expertise. If the professional does not currently have the expertise necessary to complete the assignment, the professional should disclose this shortcoming to the employer or client. The client or employer may decide to pursue the assignment with the professional after time for additional training, to pursue the assignment with someone else who has the required expertise, or to forego the assignment. A computing professional's ethical judgment should be the final guide in deciding whether to work on the assignment.

2.7 Improve public awareness and understanding of computing, related technologies, and their consequences.
Computing professionals should share technical knowledge with the public, foster awareness of computing, and encourage understanding of computing. Important issues include the impacts of computer systems, their limitations, their vulnerabilities, and opportunities that they present. Additionally, a computing professional should counter false views related to computing.

2.8 Access computing and communication resources only when authorized to do so.
No one should access another's computer system, software, or data without permission. A computing professional should have appropriate approval before using system resources unless there is an overriding concern for the public good. To support this principle, a computing professional should take appropriate action to secure resources against unauthorized use. 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.

2.9 Design and implement systems that are robustly and usably secure.
Breaches of computer security cause harm. It is the responsibility of computing professionals to design and implement systems that are robustly secure. Further, security precautions are of no use if they cannot or intentionally will not be used appropriately by their intended audience in practice; for example, if those precautions are too confusing, too time consuming, or situationally inappropriate. Therefore, the design of security features should make usability a priority design requirement.

3. PROFESSIONAL LEADERSHIP PRINCIPLES.

In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. These principles generally apply to organizations and groups, as well as their leaders.

A computing professional acting as a leader should...

3.1 Ensure that the public good is the central concern during all professional computing work.
The needs of people—including users, those affected directly and indirectly, customers, and colleagues—should always be a central concern in professional computing. Tasks associated with requirements analysis, design, development, testing, validation, deployment, maintenance, retirement, and disposal should have the public good as an explicit criterion for quality. 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 the social responsibilities of members of an organization or group.
Technical organizations and groups affect broader society, and their leaders should accept the associated responsibilities. Organizational 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 all computing professionals in meeting social responsibilities and discourage tendencies to do otherwise.

3.3 Manage personnel and resources to enhance the quality of working life.
Leaders should ensure that management enhances, 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 in the Code.
Leaders should ensure that organizational policies are consistent with the ethical principles in the Code, are clearly defined, and are effectively communicated to all stakeholders. In addition, leaders should encourage and reward compliance with those policies, and take appropriate action when policies are violated.

Leaders should verify that processes used in the development of systems protect the public good and promote the dignity and autonomy of users. Designing or implementing processes that deliberately or inadvertently 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 learn and be accountable for the scope, functions, limitations, and impacts of systems.

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 models, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and the contexts in which they are deployed, and other issues related to the complexity of their profession.

3.6 Retire legacy systems with care.
Computing systems should be retired when it is judged impractical to continue supporting them. System developers should take care when discontinuing support for systems on which people still depend. Developers should thoroughly investigate viable alternatives to removing support for a legacy system. If these alternatives are not practical or unacceptably risky, the developer should assist stakeholders' graceful migration from the system to an alternative. When system support ends, stakeholders should be notified of the risks of their continued use of the unsupported system.

System users should continually monitor the operational viability of their computing systems, accepting the timely replacement of inappropriate or outdated systems. The primary consideration must be the impact on stakeholders, who should be kept informed at all times.

3.7 Recognize when a computer system is becoming integrated into the infrastructure of society, and adopt an appropriate standard of care for that system and its users.
When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have a responsibility to be good stewards of these socially integrated 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. 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. As the level of adoption changes, there are likely to be changes in the ethical responsibilities of the organization or group. 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. Each ACM member should encourage and support adherence by all computing professionals regardless of ACM membership.

4.2 Treat violations of the Code as inconsistent with membership in the ACM.
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. Possible actions also include reporting the violation to the ACM, which may result in remedial action by the ACM up to and including termination of the violator's ACM membership.

Authors

Don Gotterbarn (chair@Ethics.acm.org gotterbarn@acm.org) is chair of the ACM Committee on Professional Ethics and Professor Emeritus in the Department of Computing at East Tennessee State University, Johnson City.

Amy Bruckman (asb@cc.gatech.edu) is a professor of Interactive Computing at Georgia Institute of Technology, Atlanta.

Catherine Flick (cflick@dmu.ac.uk) is a Senior Lecturer in Computing and Social Responsibility at De Montfort University, Leicester, U.K.

Keith Miller (millerkei@umsl.edu) is the Orthwein Endowed Professor for Lifelong Learning in the Sciences College of Education, University of Missouri, St. Louis.

Marty J. Wolf (mjwolf@acm.org) is a professor of Computer Science at Bemidji State University, Bemidji, MN.