



Association for
Computing Machinery

Advancing Computing as a Science & Profession

The Code

ACM Code of Ethics and Professional Conduct

Affirming our obligation to use our skills to benefit society

- General Ethical Principles
- Professional Responsibilities
- Professional Leadership Principles
- Compliance with the Code
- Case Studies
- Using the Code



ACM Code of Ethics and
Professional Conduct

CODE 2018 INTERNATIONAL TASK FORCE

Executive Committee

Don Gotterbarn, *Chair*
Bo Brinkman
Catherine Flick
Michael S. Kirkpatrick
Keith Miller
Kate Vazansky
Marty J. Wolf

Project Task Force

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
Julia Stoyanovich
Les Waguespack

ACM COMMITTEE ON PROFESSIONAL ETHICS

Don Gotterbarn, *Co-Chair*
Marty J. Wolf, *Co-Chair*
Florence Appel
Bo Brinkman
Karla Carter
Catherine Flick
Fran Grodzinsky
Kai Kimppa
Michael S. Kirkpatrick
Anthony Lobo
Keith Miller
Denise Oram
Thomas Owens
Norberto Patrignani
Simon Rogerson
Kate Vazansky

ACM COUNCIL

President

Cherri M. Pancake

Vice President

Elizabeth Frances Churchill

Secretary/Treasurer

Yannis E. Ioannidis

Past President

Alexander L. Wolf

Publications Board Co-Chairs

Jack Davidson and Joseph A. Konstan

SIG Governing Board Chair

Jeff Jortner

Members-at-Large

Gabriele Anderst-Kotsis, Susan T. Dumais,
Renée McCauley, Claudia Bauzer Medeiros,
Elizabeth D. Mynatt, Pamela Samuelson,
Theo Ezell Schlossnagle, and Eugene H. Spafford

SGB Council Representatives

Sarita Adve and Jeanna Neefe Matthews

ISBN 978-1-4503-6626-7

DOI 10.1145/3274591

Copyright © 2018 by the Association for Computing Machinery, Inc. (ACM)

Letter from the President



Computing professionals have a profound impact on both public and private life. Part of ACM's role is to guide computing's impact in order to better the world. As a professional organization, ACM identifies who we are by what we value. The ACM Code of Ethics and Professional Conduct clearly states what is essential to professional life. The Code is a contract among ourselves as professionals, as well as a public statement of our understanding of the responsibilities the profession has to the larger society that it serves.

With computing technology so interwoven into the fabric of daily life, the work that computing professionals do is essential to ensuring that technology is used to improve the lives of all people. Computing professionals also are the first line of defense against the misuse of technology. Our collective understanding of computing systems puts us in a position to protect sensitive information and ensure that systems integrate in ways that are appropriate, safe, and reliable. Society needs to be assured that we are committed to ethical conduct as the foundation of our work. That need has become the personal responsibility of every professional in our industry.

When the ACM Code of Ethics was last updated in 1992, many of us saw computing work as purely technical. The World Wide Web was in its infancy and people were just beginning to understand the value of being able to aggregate and distribute information widely. Today, we find ourselves in situations where our work can affect the lives and livelihoods of people in ways that may not be intended, or even be predictable. This brings a host of complex ethical considerations into play.

The ACM Code of Ethics is designed to help guide the aspirations of all computing professionals in doing our work. It acknowledges that ethical decisions are not always easily arrived at, and exhorts us, as professionals, to develop not only our technical abilities but our skills in ethical analysis as well.

This booklet, with both the Code and examples of applying the Code, is just the starting point, though. ACM's Committee on Professional Ethics has created a repository for case studies showing how ethical thinking and the Code can be applied in a variety of real-world situations. The "Ask an Ethicist" blog invites people to submit scenarios or quandaries as they arise in practice. Efforts are underway to develop ways to incorporate ethical considerations throughout the computer science curriculum, at levels from primary through graduate school.

The ACM Code of Ethics and Professional Conduct begins with the statement, "Computing professionals' actions change the world." The participation of professionals from around the world in developing the ACM Code of Ethics demonstrates that the global computing community understands the impact our work has—and that we take seriously our obligation to the public good.

Cherri M. Pancake
ACM President

A Guide for Positive Action



Computing advances in the 21st century have intensified the depth and breadth of the field's impact on society. Computing now shapes and defines the structures of society, interacting with and producing new socio-technical structures. Computing is no longer merely a support structure for doing complex calculations. It influences the essence of our being, running insulin pumps and pacemakers, managing our friendships, and identifying who should be punished, promoted, and hired. The roles and responsibilities of computing professionals have thus also undergone profound transformations that are reflected in this update to the ACM Code of Ethics and Professional Conduct.



As a rapidly changing and complex field, computing requires a high level of technical skill. High-speed and high-capacity communications facilitate local decisions that have a global impact on all aspects of society, including individual citizens. Fortunately, most of our ethical decisions are almost automatic, and consist of applying ethical decision skills we learned in our formative years. Yet, due to computing's role in changing society and the nature of human interaction, we need to revisit those ethical standards to clarify how they apply to the decisions of computing professionals. The complexity of computing systems often leads to a narrow focus on technical requirements, potentially missing the needs of some stakeholders. A book reading app may meet the requirement of enlarging font size for the visually challenged, but fail to consider the user when the instructions to achieve this effect are in a tiny font. In this example the system is an ethical failure, although it meets the technical requirement.

The change in the nature of computing's impact means that every decision requires us to identify a broader range of stakeholders and consider how to satisfy our obligations to them. A primary function of the Code is to help computing professionals identify potential impacts and promote positive outcomes in their systems. It also informs the public about important professional responsibilities and educates practitioners on the standards that society expects them to meet. Further, it makes clear to aspiring computing professionals what their peers strive for and expect of each other. As a reflection of the collective conscience of the computing profession, it encourages professionals to undertake positive actions and to resist pressure to act unethically.

The Code, like many modern codes, provides ethical principles that are to be taken as a whole. Considering a single principle often leads to incomplete responses to complex questions. Used holistically, the Code is an inspiring guide. But keep in mind that using it this way requires professionals to make ethical judgments about how various possible actions are consistent with (or conflict with) the Code's principles and, thus, expands the meaning of professionalism beyond mere technical competence.

Before you read the Code, call to mind a recent project. Use the Code to help you identify facts, stakeholders, and obligations that you might not have considered previously. Use the principles as springboards to different alternatives for decisions you made. Then ask yourself how that project could have made a more positive impact.

Don Gotterbarn and Marty J. Wolf

Co-Chairs, ACM Committee on Professional Ethics

The Code

ACM 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. The ACM Code of Ethics and Professional Conduct ("the Code") 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 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 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.

All people are stakeholders in computing.

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. In either case, ensure that all harm is minimized.

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.

Honesty is
an essential
component
of trust.

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.

Make a positive impact.

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.

Computing is a
service to society.

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.

Consistently
support the
public good.

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.

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.

Support ethical
conduct of all
computing
professionals.

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 membership in the ACM.

Each ACM member should encourage and support adherence by all computing professionals regardless of ACM membership. ACM members who recognize a breach of the Code should consider reporting the violation to the ACM, which may result in remedial action as specified in the ACM'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. This Code and its guidelines were adopted by the ACM Council on June 22, 2018.

This Code may be published without permission as long as it is not changed in any way and it carries the copyright notice. Copyright © 2018 by the Association for Computing Machinery.