

Code of Business Conduct

Version 5.7
February 2026

Table of Contents

- I. About Our Code: Why It Matters* 3**
- II. Our Values* 3**
- III. Our Business Relationships* 4**
 - 1. We take ethics and compliance seriously** 4
 - Scope and compliance4
 - Annual certification required4
 - Your responsibilities5
 - 2. We are trustworthy when conducting business**..... 5
 - Follow acceptable contracting practices to prevent side agreements5
 - Signing Authority6
 - Facilitate accurate financial disclosure and reporting7
 - Maintain business records properly7
 - 3. We follow the letter and spirit of the law** 7
 - Uphold applicable anti-corruption and anti-bribery laws7
 - Follow gift, entertainment, and hospitality guidelines8
 - Deal honestly with public or government officials9
 - Know the law when working with government customers or heavily regulated industries9
 - Promote fair competition10
 - Safeguard the privacy of personal data10
 - Our privacy principles regarding personal data13
- IV. Our Community* 14**
 - 4. We believe in social responsibility** 14
 - Be a good corporate and world citizen14
 - Dedicating your time and money15
- V. Our People* 15**
 - 5. We avoid conflicts of interest** 15
 - Avoid insider trading17
 - Report foreign boycott and embargo requests18
 - 6. We protect the company’s assets and reputation** 18
 - Use company assets and systems appropriately18

Post on social media responsibly19

VI. Our Company.....23

7. We promote a respectful workplace..... 23

8. We foster a safe and healthy work environment..... 24

9. We ask questions and report concerns 25

10. Final reminders 28

I. About Our Code: Why It Matters

This Code defines expectations of how we conduct business ethically and clarifies what is and is not acceptable behavior to maintain our personal and professional integrity. The Code helps us navigate the complex world of business and ethics by translating our values into appropriate decisions and behavior.

The Code applies to everyone in the Sitecore community: employees, contingent workers, contractors, officers and directors. It holds us all to the same standards, ensuring fairness and consistency across our business and ensuring we comply with company policies and applicable laws.

The Code does not list every legal or ethical issue you may face, but when used in conjunction with our company policies and procedures as well as common sense and good judgment, it creates a common framework for decision making and serves as a reference to help solve ethical dilemmas. Please note that violations of the Code may lead to disciplinary action, up to and potentially including termination of employment.

II. Our Values

Keep the Main Thing the Main Thing	We focus on accomplishing our most important goals. From focus comes simplicity.
Get It Done	We don't let perfect be the enemy of the good. We think about one-way and two-way doors.
Run It Like You Own It	We embrace ownership, accountability, and determination to achieve our goals.
Every Experience Matters	We care about how we show up, how we work together, and how we succeed together.

III. Our Business Relationships

1. We take ethics and compliance seriously

This Code provides guidance about business behavior expected of each member of the Sitecore community as you work and interact with fellow employees, customers, suppliers, service providers, business partners, and other stakeholders worldwide.

The Code supports our core values and policies. Issues covered by the Code may also be covered in additional local, regional, or departmental policies or handbooks. Employees can find a comprehensive list of policies on [Sitecore's intranet](#). Of course, the Code and the policies cannot answer every question or address every possible business situation. We expect you to use good judgment and seek guidance when you have questions about the appropriate course of action.

Scope and compliance

The Code applies to all employees, officers, directors, contingent workers, and independent contractors ("you" or collectively "personnel") of Sitecore Holding II A/S and its affiliates worldwide (collectively, "Sitecore"). To the extent allowed by law, aspects of the Code also apply to consultants, service providers, suppliers, and others who do business with us. Please note that simply because the Code applies, it does not create an employment relationship with Sitecore that would not otherwise exist. Each of us has a responsibility to uphold the Code.

Annual certification required

All personnel are required to review, understand, certify and comply with the Code. The Code is regularly updated based on our dynamic business environment and changing laws and regulations. You must certify every year to ensure you are familiar with the most recent version of the Code and to remind you that the Code is a resource that you can use all year long. You will be enrolled once annually in Code of Business Conduct training, during which you will complete your annual Code certification. Additionally, as part of the onboarding process, new hires are required to complete the Code certification and other mandatory training when they join Sitecore. Thereafter, new hires are required to participate in the annual Code training and certification.

Your responsibilities

Our business success depends on our ability to build trusted relationships based on respectful and professional business dealings with Sitecorians, customers, vendors, and others. This means that you have a responsibility to:

- Promote a respectful workplace
- Ask questions and report concerns (including anonymously via the Reporting Hotline if you prefer)
- Conduct business with honesty and integrity
- Follow the letter and spirit of the law
- Protect the company's assets and reputation

Ultimately, we count on you to apply good judgment and to seek guidance, as appropriate, before taking action.

2. We are trustworthy when conducting business

Follow acceptable contracting practices to prevent side agreements

Sitecore contracts with customers and other parties only through formal, written agreements that have been approved by Legal, Finance and, when applicable, Security, and have been executed by authorized signatories, as further described in the [Contract Approval and Signature Policy](#) and the [Procurement Policy](#).

Side agreements are strictly prohibited. Side agreements include any commitment, whether verbal or written (including by e-mail), that is not explicitly written into the deal documentation. Examples include:

- Modifying payment terms (including delaying PO issuance)
- Promising that Sitecore will or will not do something that is contrary to the written agreement
- Promising something in the future that cannot otherwise be guaranteed (upgrades by a certain date, fixed pricing, etc.)

Side agreements can substantially change the terms of the original agreement and potentially expose Sitecore to a risk of breaching the agreement and impacting the agreement's accounting treatment. Any modifications to an original agreement must be reflected either in: (1) a new written agreement, or (2) a written amendment to the original agreement, either of which must be properly approved and executed by an authorized signatory.

These contracting principles also apply to consultants, sales representatives, and other third parties that Sitecore hires to provide services and to act on our behalf. Our relationships with all third

parties must always be appropriate, to our business, lawful, and documented, wherever in the world they occur. Commissions, fees, and discounts must be set forth in a written agreement that includes the services provided and should never exceed amounts that are reasonable and customary in our industry. Payments may only be made against an accurate and complete invoice, and never in cash.

Signing Authority

Sitecore enters into binding agreements only through individuals who are formally authorized to do so. Every signed document, whether related to customers, suppliers, partners, employees, regulators, or corporate governance, creates legal and financial obligations for the relevant Sitecore entity. Signing authority must therefore be confirmed before execution.

Authority to bind a Sitecore entity exists only where it has been formally granted through:

- Appointment as a registered Director, Officer, or General Manager of the relevant entity; or
- A valid and current Power of Attorney that expressly covers the relevant entity and type of document.

For clarity, approval to proceed with a transaction is separate from authority to sign on behalf of a Sitecore entity.

Job title, seniority, prior practice, business urgency, verbal approval, or email confirmation do not in themselves confer signing authority. To support compliance with these requirements, Sitecore maintains internal governance tools, such as the [Directors & Officers Overview](#) and the [Signature Matrix](#), which must be used to confirm signing authority. Where the [Signature Matrix](#) applies, the signer must also confirm that the applicable value thresholds, entity, and document type are within scope. If there is any uncertainty regarding authority, Legal must be consulted prior to execution.

No employee may sign, execute, accept, or otherwise bind Sitecore to any agreement, amendment, statement of work, order form, change order, letter, commitment, term sheet, side letter, or settlement, or click “accept” to online terms, unless the employee has confirmed signing authority and obtained all required internal approvals under the [Contract Approval and Signature Policy](#) and, where applicable, the [Procurement Policy](#). This includes electronic signatures and any action that signals acceptance, such as clicking “I agree”, sending an email acceptance, or instructing a third party to proceed on Sitecore’s behalf.

Did you know?

Signing or accepting terms without proper authority risks unenforceable agreements, unapproved commitments, inaccurate financial reporting, audit findings, and regulatory or compliance exposure. In some jurisdictions, unauthorized signatories face personal liability. Confirming signing authority protects Sitecore’s assets, supports accurate financial reporting, and reinforces ethical and

compliant business practices. If you are unsure, stop. Contact Legal before you sign or accept any terms.

Facilitate accurate financial disclosure and reporting

As a global company, Sitecore must comply with various laws, regulations, and reporting obligations, as well as applicable statutory laws and regulations for local country financial and tax reporting. Sitecore must disclose full, fair, accurate, timely, and understandable information regarding our business, financial condition, and results of operations to our shareholders and debtholders as well as to statutory agencies. Accordingly, you must maintain accurate business records, respect all internal controls, and cooperate in all internal and external audits.

If you become aware of records that may be inaccurate, report the situation immediately to Finance or Legal, or via the Reporting Hotline. We do not support or condone preparing false records under any circumstances. If you have concerns regarding accounting or auditing matters, you should report them as specified on page 31 (We ask questions and report concerns).

Maintain business records properly

Sitecore is responsible for ensuring that its business records are created, managed, and disposed of properly. An effective, efficient records management program allows us to meet our business needs and to comply with all legal and regulatory obligations.

You are responsible for periodically reviewing the records in your possession and assuring you are in compliance with the [Record Retention and Disposal Policy](#), which contains guidance and a schedule for the destruction of records. Local laws regarding record retention and disposal may vary. Please contact Legal for more information.

Did you know?

Business records may include financial reports, personnel files and reviews, business or product plans, contracts, requests for proposals, customer lists, and more. Depending on its content, an email may also be a business record. If you are unsure whether something is a business record, please contact Legal.

3. We follow the letter and spirit of the law

Obeying the law, both in letter and in spirit, is the foundation of our ethical standards. As a worldwide company, Sitecore must act in accordance with the applicable laws and regulations in all countries where we do business. Where the Code or company guidelines differ from local laws or regulations, we must always follow the higher standard. If you believe the requirements of the Code conflict with local law, please consult Legal.

Uphold applicable anti-corruption and anti-bribery laws

Sitecore is committed to acting ethically as a good corporate citizen and with integrity in all of our business relationships. We expect you to act honestly and ethically in all dealings with customers, suppliers, business partners, government officials, vendors and any other business in Sitecore's supply chain consistent with our [Anti-Bribery and Anti-Corruption Policy](#). Sitecore has zero-tolerance for bribery or corruption. You may never give or promise to give anything of value directly or indirectly to any third party in connection with any Sitecore business to assist Sitecore in obtaining an improper business advantage, whether or not any benefit is received.

Additionally, any third-party, agent, or intermediary acting on Sitecore's behalf is also prohibited from offering, giving, or accepting bribes.

Follow gift, entertainment, and hospitality guidelines

We look for opportunities to build business relationships, but we never offer or accept inappropriate gifts or anything else of value to influence business outcomes. Business courtesies, such as modest meals or a nominal gift during the holiday season, can promote good will and strengthen business ties. However, we must never compromise our integrity.

This means we:

- Never offer or accept gifts, entertainment, or anything else of value if it appears to obligate someone to act or reciprocate in a certain way
- Never offer or accept anything of value if it appears to violate the policies or core values of Sitecore or the other party
- Never offer or accept cash or cash equivalents, except for specific incentives of nominal value offered through an approved company program
- Offer or accept meals only when they serve a legitimate business purpose and are not considered extravagant by local custom
- Offer or accept gifts only if they are of nominal value, generally less than EUR 150 / USD 175, though appropriate amounts may vary by jurisdiction. Contact Legal to confirm.
- Never accept gifts of any value from customers or current/potential vendors if we are involved in a license or service deal or engaged in procurement with them.

Generally, you should refrain from giving gifts to, or accepting gifts from, any third party who is doing business with, or who wishes to do business with Sitecore. Local customs may require that you exchange gifts; however, you must first obtain approval from your manager. A gift may only be exchanged in accordance with Sitecore's policies and the policies of the other party. Additionally, the nature and cost of any gift you give must be accurately recorded in our books.

You may accept and offer infrequent business meals and entertainment, provided they are not extravagant, or of a nature that might create the appearance of impropriety.

Never give or accept a loan of any amount without the prior written approval of the Chief Financial Officer and the Chief Legal Officer.

For additional information regarding acceptable and unacceptable gifts, entertainment, and other hospitality, as well as the related approval process, please refer to [Sitecore's Travel and Expense Policy](#) and [Sitecore's Anti-Bribery & Anti-Corruption Policy](#). Contact Finance or Legal to discuss and resolve ambiguous situations.

Deal honestly with public or government officials

Various local laws including the UK Bribery Act, the U.S. Foreign Corrupt Practices Act and Sapin II Law prohibit offering, promising, or giving anything of value to a public or government official. If you have any interactions with public or government officials, it is important that you know the laws and regulations that apply to those interactions. Laws in most countries prohibit or restrict government officials or employees of government agencies from receiving payments, entertainment, or gifts. This is outlined in greater detail in our [Anti-Bribery & Anti-Corruption Policy](#).

Did you know?

That the term "government official" includes various jobs and positions, including:

- Police, military, or immigration officers
- Executives and other employees of a state-owned business, such as a national oil company, state-owned refinery, national airline, or national railway
- Individuals who work for public international organizations such as the United Nations, the International Monetary Fund, or the World Bank
- Professors employed by a state university
- Any person acting in any official, administrative, or judicial capacity for, or on behalf of, any government

Know the law when working with government customers or heavily regulated industries

When a government or public entity is our customer, or our customer operates within a heavily regulated industry (such as healthcare or banking), Sitecore is subject to unique requirements that are considerably stricter than when we work with other commercial customers. A violation of these requirements can lead to serious issues. If your work involves a government customer or a customer in a heavily regulated industry, you are responsible for knowing the specific requirements that apply. Always ask your manager or contact Legal if you are unclear about what is required.

Promote fair competition

We follow laws designed to preserve free and open competition, often referred to as “antitrust laws.” Generally, applicable antitrust laws prohibit the following conduct:

- Price fixing, which includes verbal, tacit, or implied agreements among competitors about prices
- Bid rigging, through which a party agrees to not bid, bid at a certain price, or submit a bid that is intentionally less favorable than a competitor’s bid
- Territorial or customer allocation, through which competitors divide or allocate customers or territories to be served
- Market division among competitors to allocate customers, territories, or products

Antitrust and trade regulation laws in various countries may differ. Any question about specific conduct or a specific situation should be directed to Legal. In addition, you should consult Legal before joining any trade association.

Remember:

Fair competition or antitrust laws prohibit discussing or otherwise disclosing the following with competitors, suppliers, or even customers:

- Pricing practices
- Discounting
- Credit terms
- Promotional allowances
- Exclusive dealerships or distributorships
- Restrictions on carrying competing products

Safeguard the privacy of personal data

Many countries have privacy and data protection laws that govern the appropriate collection, use, storage, sharing and deletion of personal data. With global affiliates across five different continents, we are entrusted with the personal data of our personnel, customers, partners, and suppliers. We take our obligation to protect personal data seriously. We comply with applicable data protection and privacy laws in all countries where we do business. We respect the privacy of all individuals and take the necessary and legally required steps to protect personal data and prevent the harm caused by unauthorized access. But it’s not just about compliance. It’s also about making sure we meet the expectations of our customers and partners, using data in a transparent way, while following

thoughtful and ethical data practices in our community. We have established a Data Governance Committee to address and oversee issues relating to privacy and personal data.

Personal data is:

Information that identifies or can be used to identify a person. Personal data can be information about customers, employees, contractors, service providers, partners, or other parties. It can include data such as:

- Civil registration, Social Security, or other government-issued ID number
- Tax ID number
- Bank account information
- Credit card information
- Home address
- Email addresses (work and personal)
- Phone numbers
- Health/medical information
- Performance records
- Salary, comp plan, and other compensation information

You have a responsibility to safeguard the privacy, confidentiality, and security of personal data and other private information in Sitecore's possession. This means we:

- Only use Sitecore authorized tools and vendors
- Share information while keeping it safe – share information via Box or using password protection
- Report any suspicious emails
- Keep your laptops and devices safe
- Don't share your passwords
- Reach out to IT or security@sitecore.com

You must follow [Sitecore's Privacy Policy](#) and our [Information Security Policy](#) to protect personal data of fellow employees, customers, suppliers, and other third parties, and prevent unauthorized use or disclosure of such information.

Protecting personal data means we:

- Respect the privacy of our fellow employees' personal data;
- Comply with all company policies and applicable privacy laws regarding information protection, as well as the collection, storage, sharing, and destruction of personally identifiable information;
- Request and retain only as much personal information as necessary, and share it only on a need-to-know basis for legitimate business reasons as permitted by law—even with colleagues;
- Delete all personal data once it is no longer needed;
- Never leave personal information unprotected;
- Are transparent about the information we collect, use, and share, as well as what we use it for and how we share it;
- Invest in and use robust information protection controls, systems, and security procedures;
- Select vendors for marketing, tech support, or other services who share our commitment to protecting and appropriately using personal information.

When providing services to our customers — be it consulting, cloud services, support, or other services — Sitecore always respects the privacy of its customers, clients, employees, and other constituents. When working on a customer site or directly with a customer's information technology resources, you must also comply with the policies and standards of both the customer and Sitecore for the protection of personal data.

I am in sales, and one of our team members has been out with an illness. One of her customers called and asked for her address to send some flowers. Can I give out her address?

We want to build strong relationships with customers, but it is inappropriate to give out the sales representative's personal information or information about the health facility where they may be receiving treatment. We must respect the privacy of our team members' personal information. You should suggest that the customer send something to the office and work with the People and Culture Team to ensure that it gets to them.

If you suspect that personal data has been used or disclosed inappropriately, or that a security breach has occurred, please contact the Privacy Team immediately (privacy@sitecore.com). The Privacy Team will take appropriate action and manage compliance with applicable laws.

I have received a message at my Sitecore email address from someone saying that they want access to all the information Sitecore has on record about them. What should I do?

In many countries where Sitecore operates, individuals may have certain privacy rights such as the right to access their personal data or request that information about them be deleted. If you receive any request, which could be from a customer, former colleague, a current employee, vendor or partner, you should forward this immediately to privacy@sitecore.com.

Our privacy principles regarding personal data

We must protect the personal data of our current and prospective customers as well as our Sitecore community of employees, contractors, partners and vendors who trust us with their personal data. We must keep this data secure, use it only for intended purposes, and follow these privacy principles:

- **Notice, choice and consent:** We provide individuals with notice and choice about the types of personal data collected and how it is processed. Individuals may choose whether to provide personal data to us, and we respect their decisions.
- **Data purpose:** To ensure lawfulness, fairness and transparency we process personal data only for the legitimate purposes of operating our company, with consent or in accordance with law.
- **Data minimization:** Sitecore will collect, process, use and store only as much personal data as we need to fulfill the purpose for which it is collected.
- **Data quality and accuracy:** We provide reasonable access, upon request, to personal data, along with the ability to review, correct, amend, or delete data shared with us. We take steps to ensure that personal data is accurate, complete, and up-to-date.
- **Data retention and disposal:** Sitecore shall not keep hold of any personal data for longer than is necessary.
- **Data security, integrity and confidentiality:** We implement and maintain appropriate technical and organizational information security controls to ensure data security protections are in place. We treat personal information as highly confidential information, subject to our highest level of data security. We transfer personal data among Sitecore affiliates who enter intra-company agreements to help ensure data rights and protections during onward transfer. Personal data will be shared with third parties only when contractually obligated to provide equivalent levels of protection.
- **Monitoring and Enforcement:** Sitecore will be accountable for its decisions to protect data. Sitecore shall ensure compliance with global data protection and information governance laws by monitoring legal developments, following best practices and ensuring that policies are consistently enforced.

IV. Our Community

4. We believe in social responsibility

Be a good corporate and world citizen

At Sitecore, we believe that making a positive difference in the world is the right thing to do and a business essential. We recognize that our success is interconnected to the well-being of our personnel, customers, partners, and the communities in which we work and live. Our focus extends beyond the products and services we offer to encompass our responsibilities as an employer, neighbor, and steward of the planet's natural resources.

Sitecore appreciates that our work impacts the world around us. That is why Sitecore constantly strives to follow global best practices regarding sustainability. As part of Sitecore's commitment to positively impacting our environment, Sitecore conducts annual assessments to determine the actions to be taken to honor and demonstrate our commitment to sustainability.

Sitecore is committed to acting ethically as a good corporate citizen and with integrity in all of our business relationships. We have implemented and enforce systems and controls to ensure slavery and human trafficking is not, to the best of our knowledge, taking place anywhere in our supply chains. To achieve this, we have established monitoring and risk management processes to ensure continuous oversight of our suppliers and ongoing compliance obligations, such as:

- This Code of Business Conduct;
- Our Supplier Code of Conduct, which all global suppliers must review and follow;
- Supplier procurement processes to ensure that prior to engagement of new suppliers, all suppliers will be onboarded in accordance with Sitecore's procurement standards. This includes legal terms and conditions in supplier agreements being reviewed by the legal team;
- Periodic audits to review and manage risks in our supplier relationships and action any instances of non-compliance; and
- Training and awareness initiatives to educate all Sitecore personnel in their responsibilities and how to report any modern slavery or human trafficking concerns.

Sitecore will continue to review our compliance, including considering our due diligence processes around slavery, human trafficking and humane working conditions, ensuring that our suppliers adhere to the same values and ethics, implementing staff training where necessary, and monitoring our effectiveness in ensuring that slavery and human trafficking is not taking place in any part of our business.

Dedicating your time and money

With Sitecorians in many countries around the world, we also seek to strengthen the communities in which we live and work. With our goal of helping people and businesses succeed, Sitecore encourages our employees to dedicate their time, talent, and generosity as community volunteers. Supporting local communities and giving donations to charities is good citizenship. It can take the form of fund-raising activities, awareness-raising campaigns, or donations of time as experts in our field.

We always want to demonstrate good citizenship, and Sitecore supports both local and global charities to help people and nonprofit organizations in need. Donations on behalf of Sitecore can, however, be seen as inappropriate, and even considered bribery if not conducted properly and with transparency. Please see below for Sitecore's key principles to apply when giving charitable donations or volunteering your time on behalf of Sitecore.

Whenever you receive a request regarding a donation, contribution, or sponsorship, ensure that such requests adhere to the Sitecore principles and guidelines as a first step. If yes, then contact your local management and Legal regarding the opportunity.

Principles for charitable donations on behalf of Sitecore

1. Donations must be legal under local law.
2. Donations may not be linked to any tender or sales process; donations must never be made to encourage the recipient, or in any way be made with the expectation of any gain, financial or otherwise.
3. Organizations must be registered with their government as a nonprofit agency.
4. Sitecore does not make donations or contributions, directly or indirectly, to political parties, organizations, or individuals publicly engaged in politics, as this can be seen as a way of obtaining unfair advantage in business transactions.
5. Sitecore does not make donations or contributions, directly or indirectly, to organizations or individuals that promote a particular religion, church, synagogue, temple, or other religious entity.
6. Sitecore does not support or benefit any group that discriminates against any groups or individuals based on race, color, religion, national origin, citizenship, age, gender, gender identity, sexual orientation, marital status, mental or physical disability, or any other classification protected by law.

V. Our People

5. We avoid conflicts of interest

We understand that you have responsibilities and interests outside of work. However, it is your responsibility to avoid situations where a conflict of interest could occur. Generally, a conflict of interest exists when you or a member of your family has professional or personal interests or activities that could affect your professional judgment or objectivity in making Sitecore-related decisions.

Conflicts of interest may not always be immediately evident. If you think you might be faced with a conflict of interest, disclose it immediately. Talk to your manager or Legal and remove yourself from any decision-making responsibilities that are related to the conflict. Failure to disclose an actual or perceived conflict of interest is a violation of the Code.

Some examples of conflicts of interest include:

- **Outside Employment:** You should not accept simultaneous employment with a Sitecore supplier, customer, developer, or competitor, or participate in any activity that supports a competitor's position or compromises Sitecore's interests.
- **Serving on a Board of Directors:** You may not serve as a director for a competitor or any entity that might create a conflict of interest.
- **Personal Investments:** Before making any investment decisions, make sure that your investments will not compromise your responsibilities to Sitecore. Typically, investments of less than 2% of the total outstanding shares in companies listed on a national or international securities exchange do not create a conflict.
- **Related Parties/Nepotism:** As a general rule, you should avoid conducting Sitecore business with, or hiring, a family member, spouse, or significant other. In cases where it is unavoidable, you must obtain prior written approval from the Chief Legal Officer and the Chief Financial Officer.
- **Romantic Relationships with Co-Workers:** As a general rule, you should avoid romantic relationships with co-workers. These are strictly forbidden between a supervisor and a direct report. And while allowed between those who do not report to one another, romantic relationships are discouraged amongst non-reporting co-workers as they can negatively impact the work environment for others.
- **Business Opportunities:** You may not use Sitecore property, information, or your position within Sitecore for improper personal gain or to compete with Sitecore directly or indirectly.
- **Political Contributions:** You may not use Sitecore's funds or assets for political campaigns or political practices anywhere in the world without the prior written approval of the Chief Legal Officer or Chief Financial Officer.

I'm a developer on the product team. Before working at Sitecore, I had my own business developing websites for small to medium sized business. Some of my

former clients want to engage my services again. Is this type of outside employment permitted?

This sounds like a potential conflict of interest. This type of paid outside engagement could be in competition with Sitecore, depending on the types of clients and the type of services you would provide, or it could interfere with your work duties depending on how much time you spend doing outside work. To ensure you avoid a conflict, Sitecorians seeking outside consulting engagements should contact Legal who will work with you to determine if a conflict exists. Additionally, should you leave Sitecore to work elsewhere, you will also have an obligation to protect the proprietary and confidential information of our Company.

Avoid insider trading

From time to time, you may have access to material, non-public “inside information” about Sitecore, our business partners or our customers. Inside information is any information not made available to the public that could affect an individual’s decision to buy, sell, or hold securities in a company.

Information or events that could be considered “inside information” include:

- Product launch dates
- New products
- Unpublished financial reports
- Changes in senior management
- Changes in product prices
- Significant new contracts or partnerships
- Decisions to expand or reduce operations
- Mergers, acquisitions, tender offers, or joint venture activity

You may never use or share inside information to trade — or influence the trading of — stock, or otherwise use or share the information for personal advantage or the advantage of others.

I was feeling generous at a family party and told my brother-in-law that our company is about to announce a huge deal with a customer. He ran out and bought stock of that customer. I’m not guilty of anything, am I?

The rules of insider trading apply not just in business contexts but with friends and family. Passing along inside information, in this case, news of the deal, to someone who then buys or sells securities based on that information is considered “tipping”. Tipping is a violation of the securities laws of many countries, and both you and your brother-in-law could be subject to prosecution.

Comply with export controls

In many countries in which Sitecore does business, laws and regulations govern imports and exports. Many of these laws and regulations restrict or prohibit the transfer or electronic transmission of software and technology to certain destinations, entities, and foreign persons. In many cases, the law requires an export license or other appropriate government approvals before an item may be shipped or transmitted electronically.

Violations, even inadvertent ones, could result in significant fines and penalties, denial of export licenses, or loss of export privileges. It is critical that you contact Legal if you are not sure about the rules pertaining to a product or the country at issue.

Report foreign boycott and embargo requests

Certain laws prohibit Sitecore from participating in any foreign boycott or embargo. We must report any requests to participate in boycotts or embargos. For additional information, including a list of high-risk countries, please contact Legal or utilize the Reporting Hotline.

6. We protect the company's assets and reputation

Sitecore spends considerable resources to develop and maintain our business assets. We all have a responsibility to ensure that Sitecore assets are not misused, misappropriated, shared with unauthorized individuals, or sold without appropriate authorization. It is particularly important to safeguard these assets when our systems are being accessed from a remote location.

Use company assets and systems appropriately

Sitecore's assets should be used for the company's benefit only. Assets may be tangible or intangible. Tangible assets include laptops, equipment, files, emails, office supplies, and photocopiers. Intangible assets include software, trademarks, intellectual property rights, trade secrets, and copyrights.

You are expected to use company email, internet, and IT systems responsibly, and exercise good judgment and integrity when creating and sending work product, email, and voicemails. Although we respect our personnel's privacy, you should not assume that your use of company computer devices or telephone equipment is private or confidential. There should be no expectation of privacy. Sitecore reserves the right to monitor company systems in accordance with local laws. Where permitted by local laws, your use of Sitecore resources constitutes consent to such monitoring.

You must follow company guidelines for protecting Sitecore's systems, including following password guidelines and incorporating Sitecore-approved virus protection. As remote working becomes more prevalent, following these guidelines becomes more important. Internet use that is not strictly company-related during business hours must be minimized. Always use emails appropriately and

for Sitecore business purposes, as the email system is owned by, and may be monitored by, Sitecore pursuant to local laws. Please see the [Information Security Policy](#) for more information.

Post on social media responsibly

We are leaders and innovators in the online marketplace. Social media enhances our ability to have honest, direct, and meaningful exchanges with our customers, our stakeholders, and our community. We respect your right to free expression on social media while protecting Sitecore's good name. As social media allows us to communicate instantly and globally with a large audience, we are also committed to ensuring that communications regarding Sitecore are accurate and maintain our brand and reputation. By holding ourselves accountable to the same high ethical standards online as in the workplace, we are doing the right thing for ourselves, our company, our customers, and our community.

When posting on social media, you should always:

- Ensure that you do not disclose confidential information about Sitecore, our customers, suppliers, or partners, such as non-public financial or operational information
- Avoid disclosing personal information about Sitecore employees, customers, suppliers, or partners
- If posting for personal use, post on your personal time using your own resources
- If posting for personal use, refrain from using any Sitecore or third-party logos or trademarks without written prior permission

When posting or commenting about Sitecore on the internet—unless you are authorized to speak on behalf of Sitecore—you must make clear that you are speaking for yourself in a personal capacity and not on behalf of Sitecore. You can do this by using a disclaimer such as “the views I express are my own and not in any official capacity for Sitecore.”

If contacted by media representatives, you must refer media requests to authorized representatives as set forth on page 27 (Refer media requests to designated representatives).

If you engage in business use of social media as part of your role for Sitecore, you must:

- Identify yourself with your name, title, and association with Sitecore
- Reference Sitecore partners, customers, or vendors only with their written consent

Whether you are acting as an employee or an individual, please think before you post.

Did you know?

Social media includes well-known sites such as X (formerly Twitter), Facebook, Instagram, LinkedIn, and YouTube. It also includes forums, chat rooms, discussion boards like Reddit, corporate or personal blogs, comment sections in online articles, and collaborative publishing sites like Wikipedia or Google Docs.

Travel and entertain responsibly

Responsible business travel and entertainment enhances our profitability and our reputation. When traveling on behalf of Sitecore, you must ensure that business travel is intended to further Sitecore's business interests, and that travel and entertainment expenditures are reasonable, prudent, and in accordance with our [Travel and Expense Policy](#). We expect you to record business entertainment and travel expenses truthfully, accurately, and completely and to follow company policy regarding use of corporate credit cards.

Did you know?

Expense report fraud includes submitting fake receipts, reporting inaccurate mileage, falsifying customer names, and fabricating business purposes for non-business expenses.

Protect confidential and proprietary information

Sitecore is committed to safeguarding all confidential information, including information we receive from our partners, customers, suppliers, and other third parties. Generally, confidential information is any material that is private or not common knowledge to others outside of Sitecore or the relevant third party.

Sitecore's confidential information is sometimes distributed to employees by members of the Leadership Team. You are not authorized to share this information externally. Posting this information on the internet, social media sites, or by emailing the information to outside parties is strictly prohibited.

When it is necessary to share Sitecore confidential information with customers, partners, or other third parties, you are responsible for ensuring that the correct confidentiality agreements are executed in accordance with our [Contract Approval and Signature Policy](#) before the information is shared.

If your job requires you to handle, transfer, process, or disclose confidential or proprietary information about personnel, customers, or suppliers, contact Legal before taking action. For information on the handling of customer information, see [Sitecore's Privacy Policy](#), [Sitecore's Information Security Policies](#) and the [Sitecore Employee Privacy Policy](#).

Do not use confidential or proprietary information, including trade secrets, for your own purposes or in any way that is inconsistent with Sitecore's interests. Most countries have laws governing trade

secrets and confidential information. There are serious legal repercussions for anyone who violates these laws by misusing Sitecore's or another person's or company's trade secrets for the economic benefit of anyone other than the owner.

Abide by your confidentiality agreements

All Sitecore Personnel sign an agreement to protect Sitecore's confidential and proprietary information, either in a standalone "Confidentiality and Intellectual Property Agreement" or as part of their employment contract terms, as applicable. Your obligation to safeguard Sitecore's confidential or proprietary information continues after your relationship with Sitecore ends. You must obtain Sitecore's written consent prior to disclosing confidential information to anyone or using confidential information to benefit anyone other than Sitecore. We take these obligations seriously.

Your responsibility to protect confidential information also applies to work you may have done before coming to Sitecore. Sharing confidential information from a former employer is unethical and can expose you and Sitecore to legal liabilities, especially if you signed a non-disclosure agreement with your previous employer.

A co-worker asked me to share customer information from my previous employer. Can I do that?

You must not disclose that information. Customer information of your former employer is considered "confidential information" and you have a duty to protect that information and keep it secret, even after leaving that job. If you disclose the information, you are breaching this Code, as well as your duty of confidentiality to your former employer (or its customer). You could also be exposing yourself and Sitecore to legal liabilities. Additionally, should you leave Sitecore to work elsewhere, you will also have an obligation to protect the proprietary and confidential information of our Company.

Protect Sitecore's intellectual property

Sitecore's dedication to innovation is what makes us successful and sets us apart from our competitors. We actively protect our intellectual property, which includes trademarks, copyrights, software code, trade secrets, patents, concepts, designs, and informational notes.

Upon joining Sitecore you signed an agreement giving Sitecore ownership of all inventions, conceptions, discoveries, improvements, ideas, works of authorship, and trade secrets created on the job or created using Sitecore's assets. Additionally, you are a steward of the trade secrets and confidential information owned by Sitecore or third parties that are entrusted to you. You are

expected to take appropriate administrative, physical, and technical measures to properly safeguard them and prevent their unauthorized access, use, or disclosure.

You are also expected to comply with all data security and data privacy policies and procedures applicable to your work at Sitecore, and to complete any required training regarding how you handle confidential information and intellectual property.

Safeguard Sitecore's trademarks and brands

Among Sitecore's most valuable assets are its trademarks and brands. To protect the value and recognition of these trademarks, we have established guidelines that specify how and when they may be used. You must follow these guidelines whenever you use Sitecore's trademarks, and whenever you review and approve the use of our trademarks by third parties, such as marketing agencies, partners, and customers. See the Trademark Usage Guidelines on [sitecore.com](https://www.sitecore.com) for more information. If you discover that a third party is inappropriately using or attributing a Sitecore trademark or brand, report it to Legal or submit your concern through the Reporting Hotline.

Sitecore respects the intellectual property rights of others. In the course of your work for Sitecore you may want to copy or use music, video, articles, newsletters or other materials created or owned by a third party. These materials are all protected by copyright and other intellectual property rights, and you must always obtain permission from the owner before any such use. Please contact Legal for assistance.

Avoid software piracy

We are dedicated to using the intellectual property of third parties appropriately and will not tolerate software piracy. All software used by employees to conduct Sitecore business must be authorized or licensed. Your company computer has been installed with approved software, and only licensed software should be installed on Sitecore computers. If you need any additional commercial software or freeware / open source, contact the Sitecore Helpdesk for authorization and licensing requirements. Making or using unauthorized copies of software constitutes copyright infringement and may expose you and Sitecore to liability. Consult the Sitecore Helpdesk Support page for more information.

Refer media requests to designated representatives

Sitecore designates specific employees to speak with the media or analysts regarding company confidential matters. Unless you are a designated employee, you must refer all inquiries from the media and financial analysts to our Chief Executive Officer, Chief Financial Officer, or Chief Marketing Officer.

You must seek approval from Legal to speak to government or law enforcement officials regarding Sitecore on any topic, except where you are reporting to, or responding to an inquiry from, a

governmental agency or entity about a suspected violation of law; in such instance, you are not required to inform the company if you make such a report or response pursuant to applicable law.

VI. Our Company

7. We promote a respectful workplace

Our employees are the key to our success and our culture. We strive to create an environment that is open and supportive. No action could be more contrary to our values than unlawful discrimination, bullying, harassment, retaliation, or other disrespectful and inappropriate behavior. Sitecore's leaders must set a strong, ethical example and create a civil, dignified, professional work environment.

Promote honest communication and our open-door policy

As Sitecorians, we value the free flow of thoughts, ideas, questions and concerns, and encourage personnel to raise work-related issues through established processes as soon as concerns arise. Sitecore will not tolerate retaliation or victimization of any kind for asking questions or raising good faith concerns.

Value diversity and equal opportunity

With employees in more than 20 countries all contributing to our success, we celebrate the diversity of our workforce. Our approach to diversity is defined by inclusiveness, belonging, respect, and fostering a culture that allows each individual to contribute to his or her fullest potential.

Sitecore is committed to making all personnel decisions based on qualifications, skills, and merit. We provide equal employment opportunities for all applicants and employees. We also make reasonable accommodations for disabled employees and other protected groups of employees and applicants, as required by law. We follow these principles in all areas of employment such as recruitment, hiring, placement, promotion, transfer, compensation, benefits, training, facilities, and social and recreational programs.

Refrain from discrimination or harassment

We prohibit discrimination or harassment based on a person's race, color, religion, national origin, citizenship, age, gender, gender identity, sexual orientation, marital status, mental or physical disability, or any other characteristic protected by local law. We seek an inclusive and diverse working environment, and our policies against discrimination, harassment and any other inappropriate conduct apply not only to Sitecore personnel, but also to our interactions with customers, vendors and business partners.

How can I identify if harassment occurs?

Harassment that violates our policies can include any unwelcome behavior that creates an intimidating, hostile, or offensive work environment based on certain personal characteristics, without regard for whether such conduct may also be a violation of local laws, such as:

- Inappropriate remarks, actions, gestures or jokes
- Sexual, racial, religious, or other inappropriate comments, innuendos or emails
- Sexual advances, flirtations, whistling, or leering
- Verbal or physical threats
- Requests or demands for sexual favors in exchange for favorable treatment
- Actual or threatened retaliation or victimization
- Displaying derogatory, demeaning, or offensive materials, photos or pictures

If you witness or experience actions that could be harassment or discrimination, please immediately speak with your manager, HR Business Partner or contact the Reporting Hotline (see page 31).

8. We foster a safe and healthy work environment

Sitecore is committed to creating a safe and healthy workplace for everyone on Sitecore premises. If local laws provide for additional safety regulations, standards, and guidelines, those can be found in your local employee handbook.

Sound safety practices are important in all our workplaces. Part of creating a safe working environment is workplace security. If you misplace or lose your identification or access badge, please email IT immediately at help@sitecore.net. Sitecore will issue you a new badge and will take necessary precautions to ensure that only authorized personnel have access to our offices and facilities.

Sitecore expects you to take reasonable care of your health and safety at work, as well as the health and safety of your colleagues. This applies to all employees, whether working on Company premises or remotely. If you have concerns for your safety or the safety of others, contact your manager or HR Business Partner. If you become aware of any actual or potential health or safety hazard, report it immediately.

Prevent workplace violence

A workplace free of violence, weapons, and other disruptive behavior keeps all employees safe and able to concentrate fully on business. Violence or other deliberate acts intended to harm other people or their property, including threatening, menacing or intimidating comments and behavior, or stalking is prohibited. We will not tolerate threats of any kind.

Sitecore strictly prohibits weapons in the workplace, including in parking lots and workspaces at customer locations. As laws about the possession of weapons on Sitecore premises can differ, contact the People and Culture Team or Legal if you have any questions.

If you become aware of any potentially dangerous situation, including threats by co-workers or outside parties, you are required to report it immediately to your HR Business Partner or any member of management with whom you feel comfortable, or via the Reporting Hotline. All threats will be promptly investigated, and if a threat is confirmed, Sitecore will take appropriate action.

IMPORTANT: In situations involving threat of imminent personal harm, you should immediately notify office building security, law enforcement, or other emergency services, as appropriate under the circumstances.

Maintain a drug-free, alcohol-free, and smoke-free workplace

Alcohol, illegal drugs, and controlled substances can adversely affect safety, productivity, reliability, and judgment. You are prohibited from consuming or being under the influence of alcohol or possessing, distributing, or being under the influence of drugs (including inappropriate or excessive use of lawful medications) while on Sitecore premises or engaging in Sitecore business, except for lawful, moderate, and prudent alcohol consumption during legitimate business entertainment.

Additionally, smoking is prohibited on all Sitecore premises, at company- sponsored off-site events, and in vehicles owned or leased by the company. Smoking is defined as the act of lighting, smoking, or carrying a lighted or smoldering cigar, cigarette, or pipe of any kind, including the act of vaping an e-cigarette. Smoking is permitted outside of Sitecore premises in accordance with local law. Please consult your local employee handbook for the policy in your office location or contact the People and Culture Team.

Act and dress professionally

We expect all employees to project a professional image, regardless of their position. Reporting to work well-groomed, clean, and wearing clothing appropriate for the nature of Sitecore's business is the corporate standard to which we must adhere. Business casual attire is generally acceptable though different standards may apply in your local office. Please contact your manager or the People and Culture Team for guidelines regarding acceptable attire for your position.

These guidelines are based on working conditions, location, hours, and the affect that your appearance has on colleagues, customers, business partners, and others who see you as a Sitecore representative.

9. We ask questions and report concerns

Raise your concerns promptly

We are committed to providing you the support and advice you need to comply with the Code, company policies, and applicable laws and regulations. When you speak up, we have an opportunity to improve, and we encourage you to ask questions and suggest improvements.

If you have any reason to believe that the Code, corporate policies, or applicable laws and regulations have been or may be violated, you are obligated to report it. Do not conduct your own investigation; report the violation immediately to any of the available resources below:

- Your manager
- Your local Finance leader
- Any member of the People and Culture Team
- Any member of Legal

Use Sitecore’s Reporting Hotline

Alternatively, you may report any workplace concern anonymously (where authorized by law) through our Reporting Hotline (“Hotline”) the following ways:

- Web: sitecore.ethicspoint.com
- Mobile: sitecoremobile.ethicspoint.com
- Phone: Please see sitecore.ethicspoint.com for a list of country-by-country local phone numbers

This anonymous and confidential Hotline operates 24 hours a day, 7 days a week. Calls are handled by non-Sitecore personnel trained as communication specialists in hundreds of languages.

When reporting, please provide as much detail as possible, including the background and history of the matter, names, dates and places. This is especially important for items raised anonymously, which are welcome but can be more challenging to investigate. If you choose to report other than through the Hotline and wish to report anonymously, please take steps to ensure your anonymity is maintained.

Sitecore **does not** prohibit anyone from reporting concerns or making lawful disclosures to any governmental authority about conduct believed to violate applicable laws. For more information, please see our [Hotline FAQ](#) and [Global Whistleblowing Policy](#).

Sitecore’s commitment to conducting business with integrity requires that we take all reports of suspected Code violations seriously, investigate them fairly and confidentially, and take action where needed.

I've seen a colleague do something that I think could be a violation, but I am not sure. Since her actions do not affect me, is it okay for me to do nothing?

No. We rely on you to report misconduct and unethical behavior, even if it does not impact you directly. An unreported violation could cause severe damage to Sitecore's reputation and put your co-workers, our customers and our company at risk. It can also have regulatory and legal ramifications. Even if you are not sure, you have a duty to report concerns and any suspected violations.

Making good decisions

When faced with a difficult ethical decision, it helps to ask yourself the questions below.

- Is it consistent with our values?
- Does it comply with our Code?
- Is it ethical?
- Is it legal?

If you answer "No" or "I'm not sure" to even one question, then stop, consider a different action, obtain help or seek guidance from others before acting or making a decision. You may also consult the resources provided in the Code.

We will not tolerate retaliation

We do not tolerate retaliation, victimization or intimidation directed against anyone who, in good faith, reports suspected misconduct, asks questions or raises concerns. You should feel safe and are encouraged to file a report or a complaint or participate in an investigation of this Code or any company policy or procedure. Our anti-retaliation policy also applies to any complaint or report of suspected wrongdoing made to — or investigated by — any governmental agency.

I reported something suspicious that turns out not to be a compliance breach — will I be penalized?

No. If you report in good faith, Sitecore's policy of non-retaliation means that no action will be taken against you, even if you are wrong or if no unlawful violation or breach was found.

Cooperate with investigations and legal proceedings

All Sitecore personnel must cooperate fully in Sitecore-authorized internal investigations and audits that may be conducted by representatives from Legal, Finance, Enterprise Technology, and People and Culture, as well as by members of our external audit and legal firms. If you reported concerns anonymously through the Reporting Hotline, you will have the option to remain anonymous to the extent allowed by law.

Legal proceedings and investigations by government or regulatory agencies, or other third parties involving Sitecore (collectively, “Legal Matters”) must be handled promptly and appropriately. You should bring all Legal Matters immediately to the attention of Legal, and you must refrain from discussing any Legal Matter with anyone inside or outside of Sitecore without Legal’s prior approval. The requirements of this subsection do not apply to providing information or testimony, in your individual capacity, to a governmental agency on behalf of yourself or co-workers where protected by applicable law.

You should retain documents relevant to any Legal Matter, as explained in the [Records Retention Policy](#). You may never knowingly destroy documents or other records pertaining to a Legal Matter without prior Legal authorization.

Please forward all external requests for information regarding Legal Matters to Legal. Legal will oversee information gathering and coordinate Sitecore’s response. When you are asked to provide relevant records, you must promptly provide them to Legal.

Definition

Reporting “in good faith” means that you have reason to believe that a violation of the Code has occurred, and that you are sincere in your attempt to provide honest and accurate information — even if the investigation determines there was no violation.

10. Final reminders

This Code serves as our guide for conducting business with integrity. It is not an employment contract, and it confers no rights relating to employment. The Code is not a complete list of our guidelines. You are expected to know and comply with all company guidelines related to your role. Violation of these company guidelines may also result in discipline, up to and including termination of your relationship with Sitecore.

Approvals and waivers

If a situation arises that requires permission from management or another person before acting, you need to raise the issue promptly to allow enough time for the necessary review and approval. There may be rare instances where Sitecore might find it appropriate to waive a provision of the Code. To seek a waiver, speak with a manager, who will consider the request in consultation with others, such as People and Culture, Finance, or Legal. Waivers of the Code require the permission of the Chief Financial Officer or the Chief Legal Officer.

Directors and executive officers who seek a waiver should address the Board of Directors. We disclose such waivers for directors and executive officers to the extent and in the manner required by law or regulation.

Revisions

Sitecore is committed to regularly reviewing and updating its policies and procedures, including this Code. Sitecore may amend the Code from time to time as it deems necessary or appropriate. You may access the most current version of the Code on [Sitecore's intranet](#).

Version No.	Owner	Last Date of Revision	Last Approved by
5.7	Employment & Compliance Legal Counsel	18/02/2026	General Counsel and SVP Legal
5.6	Employment & Compliance Legal Counsel	18/06/2025	General Counsel and SVP Legal
5.5	Legal	20/02/2025	CHRO
5.4	Legal	09/05/2024	Chief Legal Officer
5.3	Legal	16/02/2024	Chief Legal Officer
5.2	Legal	06/10/2023	Chief Legal Officer
5.1	Legal	24/08/2023	Chief Legal Officer

Sitecore ethics and compliance resources

At Sitecore, we value your commitment to being an honest and ethical member of our team. Part of that commitment is to follow the guidelines in this Code as well as company policies and the law. If you are ever unsure about what to do, ask someone. We are all responsible for asking questions and reporting any suspected or actual violations of the Code or company policies.

Resources include:

- Your manager
- Your local Finance leader
- Any member of the People and Culture Team
- Any member of the Legal Team

If you wish to remain anonymous, you can share your concern via the Reporting Hotline:

- Web: sitecore.ethicspoint.com
- Mobile: sitecoremobile.ethicspoint.com
- Phone: Please see sitecore.ethicspoint.com for a list of country-by-country local phone numbers

Here is a guide of where to go, depending on your type of inquiry:

- For suspected violations of People and Culture Team policies or employment laws, contact your HR Business Partner
- For suspected violations of the Code of Business Conduct, policies, or laws, speak to Legal
- For concerns or complaints regarding accounting or auditing matters, speak to the Chief Legal Officer or report them to the Chairman of the Board or the Chief Financial Officer

Nothing in the Code or any Sitecore policy is intended to restrict or prohibit you from reporting to, or responding to an inquiry from, a governmental agency or entity about a suspected violation of law, and you are not required to inform the company if you make such a report or response.

By signing below, I acknowledge that I have read, understand and agree to follow Sitecore's Code of Business Conduct.

Name

Date