CODE OF ETHICS

sas

At SAS, we work hard to build an environment that fosters trust and creativity at all levels of our business. We also strive to meet the highest ethical standards of behavior in our relationships with employees, customers and Business Partners. SAS is known for both its innovative software and its curious, passionate people that help bring it to life. And SAS employees are essential to maintaining this culture and delivering the most trusted analytics to our customers.

SAS believes in doing the right thing – as a company and through its employees. The SAS Code of Ethics outlines the core values that we share and was created to help employees with resources to navigate potential challenges at work. We hire the most authentic, accountable employees in the industry, and we trust them to make good decisions. We encourage employees to never be afraid to ask questions or raise concerns.

By working together, we can ensure SAS continues to be a company of high integrity with a world-class workplace culture.

Jim Goodnight
CEO

NOTE: The SAS Code of Ethics ("Code") was revised in 2020. Revisions were made to restructure and simplify the Code, but do not change the lessons of integrity from earlier versions. SAS leadership remains committed to a culture of compliance.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

1
OVERVIEW

1.1
Why We Have a Code

SAS has been listed as a Great Place to Work for more than 20 years in numerous countries. Since our integrity is an essential component in creating a great working environment, this Code of Ethics serves as our integrity blueprint.

We understand that employees may face challenges in the workplace and seek guidance on how to respond. The SAS Code of Ethics ("Code") can help. The Code outlines SAS' expectations for our employees in many different situations and is designed to help them determine the best way to respond. In addition, the Code builds upon many of the values inherent in SAS' culture: being curious, accountable, authentic and passionate. The Code may not answer every question but can provide guidance or a pathway for answers.

1.2
Who is Covered Under the Code

Employees: The Code applies to all employees, including every full- and part-time employee at every level of SAS, and every third party who accesses SAS systems or facilities. The Code applies to all subsidiaries, representative offices, field offices or any other entity owned by SAS, and the employees and third parties of such entity. We expect every employee to review the Code and use it to make decisions that would make us proud.

Managers: While we each have a responsibility to be curious and ask questions, managers accept additional responsibilities for fostering an ethical work environment. Managers are role models and should set a good example. Managers should take concerns from employees seriously and escalate them promptly. They should also reward and acknowledge employees' ethical behavior. Human Resources maintains resources for managers to facilitate preserving integrity at SAS.

SAS expects our Business Partners to follow the SAS Business Partner Code of Conduct. A Business Partner is any supplier, vendor, consultant, subcontractor, reseller or other third-party representative acting on SAS' behalf or conducting business with SAS, including, without limitation, any person or entity engaged to sell, resell or assist in selling or reselling, any SAS® products or services in exchange for a fee, commission or other compensation.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

1.3
How to Make a Good Decision

If employees are faced with a choice of actions and are not sure which action to take, they should ask:

- Is this action consistent with our Code?
- Is this action legal?
- Does the action follow SAS policies and processes?
- Does the action benefit SAS as a whole (not just a certain individual or group)?
- Would they be comfortable if their actions were made public?

If employees can answer "yes" to all of these questions, then the action is probably ok. If the answer is "no" or "maybe" to any of these questions, further guidance may be needed.

Employees should contact any of these resources for additional guidance:

- Their manager.
- Local legal counsel.
- Legal Ethics and Compliance.
- Ethics helpline.

1.4
Report Concerns Without Fear

Make a Report or Ask a Question

We strive to create the best possible working environment for our team and our customers. Failure to comply with our policies or the law can lead to severe repercussions for SAS and individuals, including fines, jail or reputational damage. Employees should trust their judgment; if they think something is wrong, they should speak up.

How Reports Are Handled

We take all employee concerns seriously. All reports to Legal Compliance are reviewed pursuant to SAS' Internal Report Review Guidelines to determine whether a policy violation occurred. The following general steps occur pursuant to the Legal and Ethics Incident and Report Response and Investigation Guidelines:

Non-Anonymous Questions and Reports

Contact:

- Their manager or a manager they trust.
- Local legal counsel or their Human Resources Business Partner.
- Members of Legal Ethics and Compliance in SAS' Legal Department via:
  - Email to Legal Ethics and Compliance.
  - Direct contact with a member of Legal Ethics and Compliance.
- Toll-free at 1-866-680-7122 from the US and Canada.

Anonymous Questions

To anonymously report a concern or possible violation of our Code of Ethics, employees can contact the Legal Ethics and Compliance Helpline or use the resources below.

- Online from the Legal Ethics and Compliance site.

Regional-Specific Reporting

- European colleagues can follow country-specific processes for reporting.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

1. Each report is reviewed by a central report coordinator who determines the nature of the report and assigns the report to the proper group for review.

2. Facts are gathered to determine whether the report is:
   a. Substantiated (facts demonstrate a policy violation most likely occurred).
   b. Unsubstantiated (facts do not demonstrate a policy violation).

   The report review team may contact the reporter for additional facts.

3. Appropriate action is taken based on the final report.

4. If appropriate, once the review is complete, the coordinator or report review team will communicate with the reporter. Communication is not possible in anonymous reports, unless the suggested generic Gmail account is used.

Confidentiality

We make reasonable efforts to only share information reported with SAS resources who have a need to know the information in order to properly investigate the report. If required by law, the information will be shared with government officials.

No Retaliation

SAS understands that it can be difficult to speak up, especially when something may be wrong. We will not retaliate against anyone who speaks up, in good faith, to report their concerns about a possible violation of the Code, SAS policies or the law. If an employee believes they are suffering from retaliation, they should follow one of the reporting avenues described herein or contained within SAS' No Reprisal, Retaliation, or Victimization Policy. As long as concerns are reported with all of the information an employee has and with honest intentions, they are protected.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

1.5
External Audits, Inspections, and Investigations

SAS will do its best to respond to and comply with all lawful audits, inspections and investigations. SAS recognizes that this course of action helps to build trust. Employees are expected to do the same. If an employee is contacted by anyone regarding an investigation or audit, they should refer the request to our Chief Legal Officer and our Senior Director of Communications immediately.

It is important for SAS to retain its records for the retention periods prescribed by applicable federal and state laws, as well as regulatory bodies. SAS expects all SAS Resources to maintain records for the periods of time prescribed in SAS' Record Retention Policy as well as any period of time directed by SAS legal counsel in connection with a specific issue.

2
ACCOUNTABILITY
to each other

2.1
Workplace Conduct

SAS has a Global Conduct Policy that is designed to complement this Code of Ethics. Both are intended to help employees navigate through ethical situations they may encounter as part of their job and to define the types of behavior we expect from SAS employees. Please see SAS' Global Conduct Policy for more details.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

2.2
Workplace Violence

SAS emphasizes employee personal safety and will not tolerate any level of violence against its employees or its workplace. Examples of violence include bullying, threats, intimidation or attempts to instill fear in others. Weapons are not permitted at work. Report any suspected threats of violence in the workplace to HR or Security and Safety.

2.3
Drugs & Alcohol

SAS does not permit its employees to work under the influence of alcohol, drugs or mismanaged over-the-counter drugs. In addition, SAS does not permit employees to consume alcohol during work hours, unless the alcohol is provided by or authorized by SAS. When acting in a professional capacity, employees are expected to use good judgment regarding alcohol and other substances at all times.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

2.4
Protection From Discrimination, Harassment, Bullying and Retaliation

At world headquarters and across all of its country offices, SAS is committed to providing an equal employment opportunity that treats all employees and applicants equally based on merit and experience – without regard to age, race, color, sex, gender, gender identity, religion, creed, ancestry, national origin, citizenship status, marital status, sexual orientation, veteran status, disability, medical condition, pregnancy or any other protected class as defined by federal, state or local law. SAS recruits, hires, trains and promotes without regard to protected characteristics and ensures that all its employment decisions are based only on valid job requirements. SAS is committed to providing a workplace free from discrimination, harassment, bullying and retaliation. Employees who experience or witness any of the above behaviors should report their concerns to their manager and/or SAS Human Resources immediately.

2.5
Diversity and Inclusion

At SAS, it's not about fitting into the culture, it's about adding to it. Diversity and inclusion at SAS are multidimensional. SAS' diverse workforce brings unique talents and inspires teams to create software that can change the world. SAS' culture blends the different backgrounds, experiences, perspectives and abilities from employees in nearly 60 countries around the world. From the technology SAS designs to the conversations shared, SAS' diversity is a creative asset. For more information, see SAS' Employees & Culture section in the CSR report.

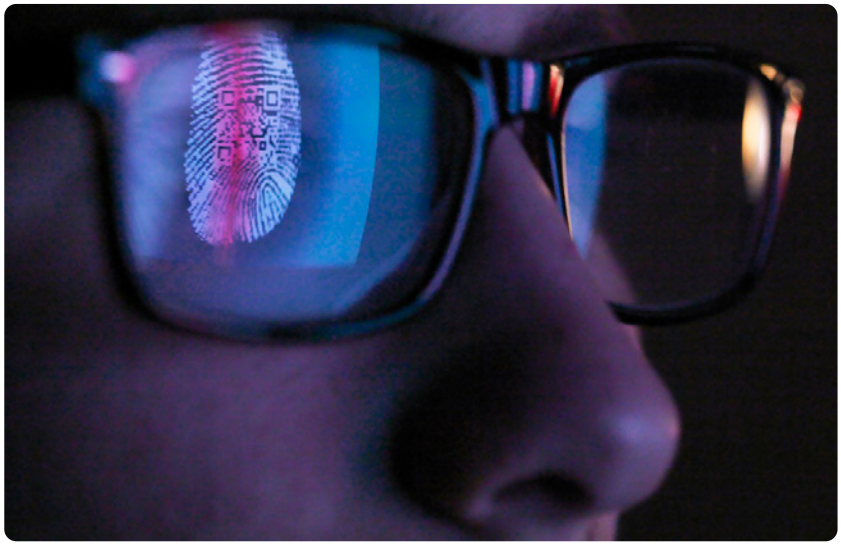
Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

2.6
Workplace Safety

Every employee has a shared responsibility to make SAS a safe and healthy place at work. If employees notice unsafe or unhealthy conditions, they should report them immediately to their manager, the Risk and Insurance Department, or Security and Safety. We have resources in place to address employee concerns and make SAS a great place to work.

2.7
Employee Data

SAS is committed to protecting an employee's privacy and identity by safeguarding any information that is provided to us as a condition of their employment. In addition, every employee is expected to protect others' personal information when the situation arises. Employees should not attempt to access their colleagues' sensitive information without specific authorization and a good reason. If an employee is responsible for sensitive information due to job requirements, they should ensure that it is protected from loss, theft or accidental disclosure. Personal information can include:



- Benefits/compensation information.
- Medical records.
- Home address, telephone numbers, email addresses or other contact information.
- Government identification number.
- Tax records and information.

If an employee has questions about protecting SAS employee data, or they need to report the actual or suspected inappropriate disclosure of data, they should contact the Privacy Office, Information Security or Human Resources groups.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

3
ACCOUNTABILITY *to SAS*

3.1
Conflict of Interest

A "conflict of interest" describes a situation where an employee's personal interest may unduly influence the employee's work for SAS. Employees should act in the best interest of SAS and avoid situations that benefit a small group or individual over SAS. Employees should avoid conflicts of interest, use good judgment, and ask managers or use other resources for help if they are unsure of the best action to take. **Employees should promptly report** any personal interests or circumstances that might constitute a conflict of interest by using the reporting procedure found in SAS' Conflict of Interest Policy.

Conflicts of interest can arise in many situations, including but not limited to:

- Personal investments in competitors or partners.
- Accepting outside employment (such as with SAS Business Partners).
- Hiring an individual with whom the employee has a personal relationship (e.g., friends, family members or former SAS employees).

3.2
Following Internal Processes/Recordkeeping/Fraud

In the course of their everyday activities at SAS, employees must be committed to following processes and policies specific to all of SAS and to their particular jobs, including but not limited to processes such as approval matrices, expense reimbursement policies, criteria for booking deals, or engaging with partners or third parties. Please consult your manager and/or contact Legal Ethics and Compliance if you have a question regarding whether a specific action violates a particular process. SAS Policies and related processes, including business-area specific standards and processes, provide additional direction. Employees are expected to follow the blueprint of the Code and the specific policies and processes that apply to the action they are taking.

Recordkeeping / Fraud

Employees should ensure their records are a truthful account of what they are recording.

Employees should follow all legislative requirements and best practices whenever creating or maintaining records. This includes all applicable accounting requirements, contract documentation, and internal controls and policies related to accounting, finance and contracts. Honesty and transparency are critical to building the trust that our customers place in SAS.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

In dealing with document retention and disposal, employees should follow SAS' Global Records Retention Policy and Records Retention and Disposal Schedule Standard along with all applicable departmental and governmental requirements. Please note employees must follow any directive which states they must not dispose of any documents from SAS Legal or external legal counsel. Effectively managing our records allows us to meet our business needs and ensure important documents are available whenever SAS needs them.

Contracting, No Side-Letters, and Signature Authority

Employees should be responsible stewards of SAS company funds and should not sign any document committing SAS to something unless the required signing authority has been secured. When making this decision, the total costs involved in a purchase should be factored in, and purchases should not be divided into smaller ones to bypass the limits of spending authority. In addition, employees may not agree orally or in writing to perform any activities or undertake any obligations on behalf of SAS without first obtaining a fully executed contract.

Money Laundering

SAS would never knowingly engage in or facilitate illegal activities, but some criminal activity, like money laundering, may not be obvious. Money laundering is a process where funds generated through criminal activity are moved through legitimate businesses to hide the criminal origin. SAS is committed to conducting business in a way that prevents the use of our business transactions by those who might abuse the law, and we comply with applicable anti-money laundering, financial crime and anti-terrorism laws.

In practice, employees should:

- Ensure Business Partners follow SAS' Third-Party Anti-Corruption Due Diligence Process and Vendor Set-Up Process.
- Be alert and report red flags in transactions to Finance or Legal Compliance. Red flags include:
  - o Large cash payments or unusual fund transfers.
  - o Customers or Business Partners who provide incomplete information or avoid recordkeeping requirements.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

3.3
SAS Property

Intellectual Property

Intellectual property (IP) must be safeguarded at all times. It can include intangible property like copyrights, patents, trademarks, design rights, inventions, systems, processes, logos, brands and other assets. All employees should help protect the company from harm and enforce its legal rights to IP to the fullest extent allowed by law.

Employee creativity is encouraged to build SAS' intellectual property. The patent team in the Legal Division can assist employees in registering and protecting any new ideas.

Source Code

SAS source code is our most valuable intellectual property. Safeguarding SAS' source code is essential to our company's continued success. Any transfer of source code must follow the Source Code Protection Standard, including:

- Following all approval processes.
- Obtaining a Non-Disclosure Agreement from SAS Legal.
- Validating export authorization with Legal Compliance Trade Counsel.

The Legal Department will provide the appropriate forms and work with you to ensure the appropriate transfer of source code.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

Trade Secrets & Confidential Information

SAS expects employees to help protect its confidential and proprietary information; without such protections it would be difficult to stay in business. Confidential or proprietary information includes a variety of information and trade secrets, most of which are not public knowledge. Trade secrets – meaning data that gives SAS an edge against competitors – can include any of the following:

- Sales programs and strategies.
- Marketing studies and plans.
- Customer records.
- Financial data.
- Pricing information.
- Software or IT detailed architecture data.
- Unpublished documentation.
- Source code.
- Information received via third-party relationships.

Physical Assets

SAS employees have many freedoms at work, but they are expected to always use company property, facilities and physical resources for their intended purposes. Any attempt to take or remove property from the company, such as documents, equipment or other belongings, violates that trust. Using company computers to harass or bully others will not be tolerated. Employees should report any actual or attempted theft, misuse or other improper activities immediately.

Computer Systems

The efficiency of our computer systems is vital for our business. We each have the responsibility to act professionally and ethically whenever we use such systems. While employees are permitted to use SAS systems occasionally for personal use, they should understand that all data recorded or transmitted into the system becomes the property of SAS. This includes all email, voicemails and company documents contained on company computers or phones. SAS trusts its employees and will only access such information in support of our legal or policy responsibilities, which may include a government request in a personnel matter.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

Representing SAS Professionally

Communications: Employees should draft emails, instant messages and other communications respectfully. Communications may be accessed or shared in unexpected ways, making it important to always speak respectfully and professionally.

Social Media: Social media dramatically affects our business no matter where we operate. Employees should be aware of the impact that comments and behavior can have on others through these networks. Therefore, employees should always behave professionally and politely when using social media on behalf of SAS.

4

ACCOUNTABILITY *to customers*

4.1 Customer Expectations

As a leader in the data analytics industry, SAS is proud of its products. Our software is designed to offer the best experience and provide excellent value to our customers. In order for our software to meet or exceed customer expectations:

- We work hard so that our products are delivered according to applicable laws and regulations.
- We maintain rigorous quality controls.
- We keep informed about industry trends.
- We ensure that our products meet their published specifications.
- We act quickly to resolve issues or conflicts. If employees have any concerns regarding our products or their quality, they should discuss them with their manager.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

4.2
Customer Data

As a company with a business built on processing data, the safety of employee, customer and Business Partner data is a priority. Customers trust SAS with all kinds of sensitive data. SAS uses physical, technical and organizational measures designed to protect personal and proprietary information against accidental or unlawful destruction, loss or unauthorized access. SAS complies with applicable data protection and privacy laws. We maintain an information security program that uses safeguards proportionate to the risks associated with the processing of the data, meaning sensitive information is subject to enhanced security measures. An example would be using encryption technology to protect sensitive data like tax records.

As a company, we:

- Provide transparent privacy policies and statements.
- Maintain secure databases to protect customer data from theft and use security techniques such as encryption when handling sensitive data. Through SAS' Credit and Debit Card Processing Standard, SAS takes measures to ensure compliance with applicable standards.
- Provide products that help our customers to protect their data and comply with laws such as the European Union General Data Protection Regulation.

4.3
Insider Trading

Employees may become aware of information regarding publicly traded companies before it is released publicly due to their role at SAS. To maintain our integrity, employees should never buy or sell securities based on material non-public ("inside") information learned because of their SAS job.

- Inside information can include material, non-public information that is important when making an investment decision. This includes financial data, unannounced product developments, etc.
- Trading on inside information is illegal and subject to prosecution if discovered.
- It is also illegal to provide such information to others to inform their investment decisions.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

5
ACCOUNTABILITY
to our community

5.1
Anti-Corruption and Fair Business

SAS believes in winning business fairly based on the quality of our products and services, never through corrupt or anti-competitive behavior.

Bribery

SAS does not tolerate bribery or corruption. A bribe is giving or receiving anything of value in exchange for an improper decision or action. Employees should never offer or accept anything of value to get business, to keep business or to gain an unfair advantage.

Acts of bribery and corruption are prohibited by the laws of the countries where SAS does business. The consequences of violating anti-corruption laws can be severe for you and SAS.

Gifts or Business Courtesies

Providing "gifts" or business courtesies can be considered a bribe in some circumstances. The term "thing of value" can refer to hospitality (e.g., travel and transport services, hotel expenses and business meals), entertainment, prizes and other business courtesies. To help employees make decisions about gift giving, SAS developed the Gift Guide for guidance when a gift is provided outside of an event. For guidance when gifts will be provided as part of an event, please see the Event Guide link within the above mentioned Gift Guide.

SAS' Gift Guide incorporates rules specific to jurisdictions.
In general, employees must only provide or accept things that are:

- Given for a bona fide/legitimate and apparent business purpose.
- Reasonable in value and appropriate in context and not a cause of embarrassment or the appearance of impropriety for SAS.
- Purely gratuitous. Purely gratuitous means the gift is not given on a "quid pro quo" basis or otherwise intended to induce the recipient to improperly grant a business or competitive advantage in return.
- Permissible under local law and the recipient organization's gift rules.
- Not in the form of cash or cash equivalents.
- Properly documented, recorded and disclosed in accordance with SAS' accounting procedures and the documentation requirements contained in SAS' Gift Guide, including documentation necessary for lobbying law disclosure requirements.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

Preferred gifts are:

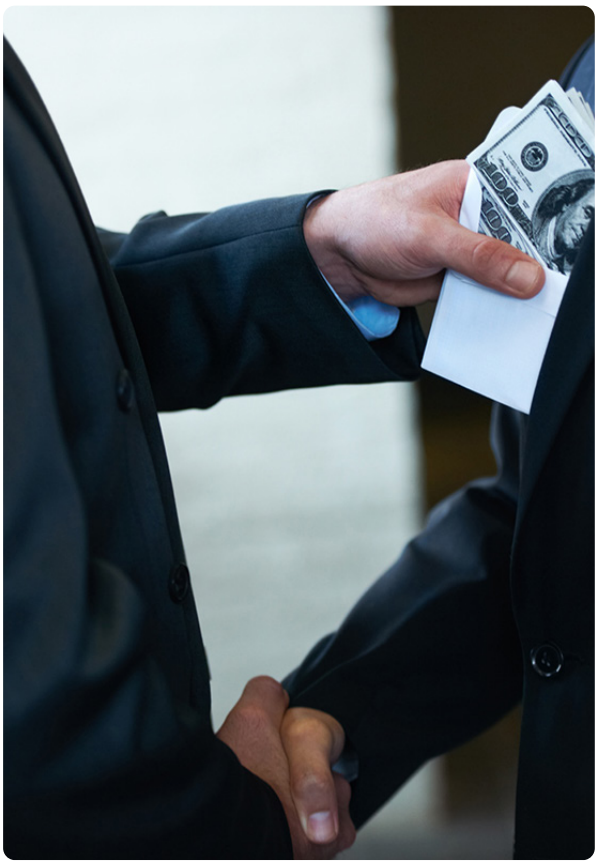
- Infrequent.
- Nominal in value (see country values in Gift Guide Matrix).
- Perishable items.
- Commemorative or promotional items bearing the SAS logo such as pens, caps and shirts.

Working with Third Parties/Business Partners

SAS and the individual employee are responsible for the acts of third parties acting on our behalf. Business Partners and other third parties may not engage in bribery or other corrupt acts on SAS' behalf. Employees must manage the work of Business Partners closely to ensure the Business Partner adheres to the standards of the Code.

In practice, employees must:

- Treat our customers and Business Partners fairly in their interactions.
- Ensure our Business Partners' accountability by informing them about SAS' Business Partner Code of Conduct and the values outlined within that document. Report any violations that you see or suspect.
- Choose Business Partners ethically and ensure Business Partners are approved through SAS' Third Party Due Diligence process. If an employee is involved in selecting Business Partners for SAS, they need to make their choice objectively, selecting them based on price, quality and the services offered. Follow all Procurement and Finance requirements.



Government Engagement

If an employee works with government personnel through their job at SAS, they may face increased corruption risks and in all cases this must be avoided. There may be pressure to use bribery to obtain government agreements in some cultures. In an effort to counter this, many countries have enacted strict gifting, engagement and procurement laws to curtail the legacy of bribery in the government sector and protect public funds.

To ensure compliance with these laws.

- Employees must follow the Gift Guide and the prior approval steps outlined there when providing anything of value to government personnel.
- Countries and sales units engaging in a focused government sales strategy must dedicate sufficient operational resources, working in conjunction with Legal Ethics and Compliance, to implement appropriate mitigation measures, depending on the local country laws, including:
  - o Lobbying or other government interaction assessment and compliance.
  - o Work restriction ("Revolving Door" and "Patronage") reviews for new employees or Business Partners with recent government history or connections.
  - o Contingent fee reviews.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

Lobbying

Lobbying is heavily regulated and may require disclosure or be subject to specific rules. Unless an employee is expressly authorized to do so, they should avoid activities that could be construed as lobbying. Lobbying covers many different types of activity, and an employee may be lobbying if their work covers:

- Contracts with legislators, regulators, executive branch or ministry officials, or other government officials.
- Efforts to influence or inform legislative or administrative actions of any kind.
- Communicating with government officials.

Employees should be especially careful when hosting government officials, legislators, regulators, political candidates, or other individuals of a political nature on SAS property. They should always seek Legal Department approval before inviting such guests. Even if the visit is authorized, you must avoid any appearance of impropriety.

Personal Political Contributions

SAS encourages employees to support the political candidates and causes of their choice. However, there are guidelines they must follow whenever making political donations.

- SAS Funds or Assets: No SAS funds or assets (including our company name) may be used to support any political activity, committee, or any candidate or government official without approval via the Sponsorship, Membership, Charitable and Political Contribution Review Process.
- Individual Funds or Assets or Political Activities:
  - Executives and registered lobbyists should report any individual political contributions to Government Relations. They need to be clear that their views are their own and do not represent SAS, especially if they are running for office.
  - Never let political activities create a conflict of interest or the appearance of one.

Employees should never be pressured to support a cause or a candidate. They are encouraged to report any such pressure. SAS is prohibited from reimbursing any employee's political contributions.

Fair Dealing and Competition

Fair Dealing: Be truthful in conversations with customers and Business Partners. Do not engage in any unfair,deceptive or misleading practices. A deceptive practice includes any leaving out of an important fact or saying something that is not true to convince someone to take action.

Competition Laws: SAS follows relevant antitrust and fair competition laws by winning business on the basis of our innovative software and customer service and not by restricting another company's ability to compete against us. In practice, this means that we expect employees to keep detailed records, accounts and documentation that reflect the decision making used in determining what is best for SAS. Employees should:

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

- Never enter into a formal or informal agreement that could restrain trade or foster anti-competitive behavior. Examples include agreements made with Business Partners or competitors, such as price fixing, bid rigging, dividing markets, etc.
- Avoid even the appearance of such an anti-competitive agreement. Even if there is no actual agreement, the appearance of such an agreement can lead to severe consequences for SAS and the employee, and therefore should be avoided.
- If anyone tries to discuss anti-competitive topics or issues, walk away immediately. Make it very clear that the employee will not participate in such discussions.

Report any incident or other type of interaction to their manager or the Legal Department immediately.

5.2
Cross-Border Business and Trade

Since SAS products are used by customers globally, we are careful to comply with the laws and regulations that govern international trade, including applicable export and import laws. The United States export laws apply to SAS, all our related entities, and the export and use of our products globally. We do not support unauthorized business with countries or third parties that are subject to trade embargoes or economic sanctions. We obtain all necessary authorization before exporting controlled technology. As a United States-based company, we cannot participate in boycotts that the United States does not support.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

Embargoes, Sanctions and Know Your Customer

Embargoes: United States law prohibits or severely restricts US companies and their foreign subsidiaries from transacting business with Belarus, Cuba, Iran, North Korea, Russia, Syria, Crimea, Donetsk and Luhansk Regions of Ukraine and other geographies. Since these restrictions may change often, SAS' Legal Ethics and Compliance department maintains a list of current embargoed/restricted geographies and information on how to check for suspicious transactions. Employees should always comply with all trade restrictions. Penalties for violating sanctions related to embargoed countries are severe and can be costly to SAS and its employees.

Sanctioned Parties and Know Your Customer Due Diligence: United States law prohibits US companies and their foreign subsidiaries from transacting business with certain entities and individuals for various reasons, including links to terrorism, drug trafficking, human rights violations or criminal activity, regardless of where the party is located. The law also prohibits certain end-uses of SAS technology. Since these restrictions and lists of persons change often, SAS' Legal Ethics and Compliance department screens for sanctioned parties and provides SAS personnel with training and information on how to conduct know your customer due diligence and check for prohibited or suspicious transactions. Employees should always comply with these trade restrictions. Penalties for violating laws related to sanctioned parties and restricted end-uses are severe and can harm SAS and its employees.

Technology Controls

If an employee's job at SAS requires them to transfer goods, services or SAS technology, they must comply with all relevant rules.

They should:

- Always provide accurate information to the customs agency for import transactions.
- Always pay all duties and customs charges owed.
- Maintain proper import and export records.
- Obtain proper licenses, classifications and export clearances whenever appropriate or required by law.

In some countries, SAS may be required to obtain advance import authorizations based on the technology in our software products.

If an employee works with SAS source code or encryption technology, they must review and understand the corporatewide Encryption Development and Use Policy.

If an employee's duties involve military (including intelligence/surveillance), national defense or national policing customers, they should complete applicable training and be familiar with the guidance available at SAS' Legal Ethics and Compliance site.

Boycotts

The United States maintains "anti-boycott" legislation that applies to a boycott of any United States ally and in general:

- Prohibits SAS from refusing to do business with any US allied person because of such a boycott.
- Prohibits SAS from cooperating with any boycott of a US ally or providing information to any boycotting country or company regarding SAS' business dealings with that ally.
- Requires SAS to immediately report any boycott request to the US government.

If an employee receives a boycott request, they must report it immediately to the Legal Ethics and Compliance Department. Failure to report boycott requests and comply with US law can lead to severe penalties for SAS and the employees involved.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

5.3
Global Citizenship

General Compliance With Laws

SAS employees, customers and Business Partners rely on our employees' integrity. Even when there is no specific mention in this Code nor policy prohibiting an employee's actions, if they know or suspect that their actions violate a law, SAS expects an employee to refrain from the action.

Human Rights

SAS' innovations come directly from its working environment and employees, and SAS cares deeply about the health and well-being of each of its employees. SAS offers employees industry-leading benefits, adheres to wage and hour laws in all jurisdictions it operates in, and fosters an inclusive culture that lets each employee do their best work.

SAS recognizes that its business has an important impact on the community and is a force for change. To accomplish its potential, SAS incorporates human rights into its business. SAS upholds human rights standards and is a member of the United Nations Global Compact. We also run a Corporate Social Responsibility program that sponsors philanthropic and environmental causes. See our Corporate Social Responsibility report and website for more information.

SAS strongly condemns human rights violations wherever they occur and works to ensure that its operations are free from those who would be complicit in such activities. This includes human trafficking, child labor violations and other rights abuses. We understand our role in helping to create a more ethical marketplace and will use our influence to ensure that any party we interact with is doing its best to eliminate the potential for abuse.

Sustainability

SAS makes every effort to be a leader in adopting environmentally sound business practices and technology into its operations. We try to be environmentally conscious in our daily work, and push initiatives to conserve energy, water and other resources on campus. Almost all of our headquarters buildings are LEED certified, and we invest in many environmentally friendly technologies to make our campus smart and efficient such as IoT tracking software, solar installations and even beehives.

We strive to set a good example by working to ensure we meet or exceed every environmental law, regulation and standard that applies to our business. See our CSR report for more detail on SAS' environmental initiatives.

5.4
Volunteering and Charity

Our company strives to support our community through charitable and philanthropic activities. SAS chooses to sponsor many different charitable causes, especially those related to STEM education and related fields. SAS encourages employees to be involved in these initiatives or any causes they are passionate about. Please see our annual Education and Philanthropy summary and Data for Good efforts.

Although SAS has made education its primary philanthropic focus, SAS believes that service to others makes the world a better place and actively encourages employees to get involved in their communities. Through its Volunteer Time Off program, SAS provides eligible employees with an opportunity to engage in meaningful and purposeful volunteerism. SAS Volunteer Time Off Policy provides details on how the program works, which allows for 20 paid hours for full time employees and 10 for part-time hours per calendar year for volunteer activities to eligible organizations described in the policy.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.

Internal policy links have been removed from this external version.
Please contact SAS Legal Ethics and Compliance for any additional information.