



Code of Conduct

STANDARD PRACTICE 150

----- PAGE INTENTIONALLY LEFT BLANK -----

150

Code of Conduct

- 1. PURPOSE 3
- 2. RESPONSIBILITY 3
- 3. NO RETALIATION 4
- 4. ETHICS 4
- 5. CONFIDENTIALITY AND CUSTOMER CARE 5
- 6. CONFLICTS OF INTEREST 5
- 7. INSIDER TRADING 5
- 8. COMPANY RECORDS 6
- 9. EMPLOYEE INFORMATION 6
- 10. PROTECTION OF COMPANY ASSETS 6
- 11. PROTECTION OF INTELLECTUAL PROPERTY 6
- 12. PROTECTION OF INFORMATION AND DATA SOURCES 7
- 13. GIFTS, FAVORS, AND ENTERTAINMENT 9
- 14. SKYWEST AND THE LAW 10
- 15. CORRECTIVE ACTION 10

1. PURPOSE

- A. The Code of Business Conduct (Code) applies to all employees, including officers, and any third party representatives (e.g., contractors, consultants, agents) of SkyWest Airlines, Inc. (SkyWest). The Code describes the ethical and legal responsibilities all SkyWest employees are expected to uphold and provides basic guidelines for conducting business on behalf of SkyWest.
- B. The Company has adopted this policy in order to discourage illegal or unethical activity and business conduct that may disrupt the business operations of the Company, to promote a climate of accountability, to facilitate compliance with all applicable laws and regulations, and to ensure no retaliation for those reporting a suspected violation.

2. RESPONSIBILITY

- A. Managers (defined as employees who supervise others) are expected to exemplify the highest standards of ethical business conduct. Managers are responsible for creating a work environment that promotes honest and ethical behavior and are required to be familiar with applicable policies and legal requirements to ensure employees receive appropriate training and guidance.
- B. Each employee is expected to make ethical decisions.
 - 1) Each employee should seek advice before problems occur and report incidents that raise compliance issues.
 - 2) All illegal or unethical conduct is prohibited regardless of the intent to benefit the Company or oneself.

3) Employees should report known or suspected violations of the Code, law, or Company policies in the following manner:

Situation:	Report to:
Workplace issues	Supervisor or Manager
Human Resources (HR) concerns or policy guidance and interpretation	Employee Relations (ER) manager or HR representative
Legal questions on behalf of the Company and misappropriation of Company assets	Director Government and Legal Affairs
Unsafe conditions, workplace hazards, and security concerns	Director Safety Policy and Security

NOTE: Typically, employees will report violations to their direct supervisor first. When the situation involves the direct supervisor, report the violation to either an appropriate manager, an ER manager, an HR representative, the Director Human Resources, or the Director Government and Legal Affairs.

3. NO RETALIATION

A. SkyWest’s policy forbids retaliation against any employee who, in good faith, reports a suspected violation of law or policy, including harassment or discrimination. Any person involved in retaliation is subject to corrective action, up to and including termination of employment.

4. ETHICS

A. Employees may make anonymous and confidential reports to the Director Government and Legal Affairs. Actions subject to reporting include irregular or fraudulent accounting, illegal activities (e.g., theft of Company property), or any activity which jeopardizes the SkyWest workplace as a productive work environment. (Refer to [Company Policy Manual SP 53 Productive Work Environment](#)).

B. Employees may submit a complaint by one of the following methods:

- 1) Registering a complaint to their immediate supervisor or any other supervisor or manager of their choice.
- 2) Phoning the toll-free Ethics and Grievance Hotline at 888.273.9994.
- 3) Reporting online at www.reportlineweb.com/SkyWestAirlines.
- 4) Writing to:

Director Government and Legal Affairs
 SkyWest Airlines
 444 South River Road
 St. George, UT 84790
 (or emailing temerson@skywest.com)

C. The employee submitting a complaint may remain anonymous. When the employee chooses to reveal their identity, the Company will not disclose that information, unless granted permission from the employee or when required to do so by law.

NOTE: All reports of irregularity should provide complete details to assist in the investigation.

D. The Director Government and Legal Affairs, or authorized designee:

- 1) Immediately reports any substantive complaint to the Chair of the Audit Committee.
- 2) Makes a general report of all complaints received to the Board of Directors on a regular basis.

- 3) Takes all necessary steps to investigate complaints and propose a solution to the Board of Directors when an error or deficiency is identified.
 - 4) Evaluates and ensures the application of the Sarbanes-Oxley Act (SOX), as appropriate.
- E. All complaints pertaining to the protection and preservation of the SkyWest productive work environment are forwarded to the Vice President People for immediate investigation. Following this investigation, all substantive complaints are resolved according to [Company Policy Manual SP 53 Productive Work Environment](#). Employees who have engaged in unethical or illegal activities are subject to corrective action, up to and including termination of employment.

5. CONFIDENTIALITY AND CUSTOMER CARE

- A. Personal information is often required from customers, including credit card information, address, flight itinerary, etc. SkyWest's policy is to use this information for Company business purposes only. Disclosures to third parties are made only in accordance with applicable law or Company policy.
- B. Employees must provide customer service that clearly demonstrates the Company's commitment to excellence and safety.
- C. Employees must show a commitment to safety and strive to give excellent customer service in all job activities.

6. CONFLICTS OF INTEREST

- A. SkyWest has a **zero tolerance** policy for any activity that creates a conflict of interest with an employee's responsibilities at SkyWest. Conflicts arise when an employee uses their position at SkyWest for personal gain, or when the employee's personal interests conflict with SkyWest's interests.
- B. All employees must avoid any actions or relationships that could conflict with, or appear to conflict with, the interests of SkyWest (e.g., an employee or family member who receives improper personal benefits including gifts, entertainment, service, or payment as a result of their SkyWest position).
 - 1) The employee must disclose in advance any relationship that might be perceived as a conflict of interest to their immediate supervisor/manager. Failure to disclose personal interests as described in this section will result in corrective action, up to and including termination of employment.
 - 2) Employees must not make, participate in making, or attempt to influence any business decisions relating to competitors, suppliers, or customers in which they have a substantial direct or indirect ownership interest. Prior to making a decision that could appear to be a conflict of interest, the employee must disclose the situation to their supervisor.
 - 3) A conflict of interest also may arise when Company business decisions involve competitors, customers, or suppliers who employ a family member of a SkyWest employee, or an individual with whom the SkyWest employee has a close personal relationship. In such instances, the SkyWest employee must not conduct Company business without first disclosing the situation to a supervisor.

7. INSIDER TRADING

- A. SkyWest is committed to promoting fair and open markets for publicly traded securities. All SkyWest employees, therefore, are prohibited from trading any securities of SkyWest or any other company on the basis of material, non-public information.

NOTE: Material information is any information a reasonable investor would consider important in making a securities-related decision.

- B. All SkyWest employees are prohibited from communicating material, non-public information to anyone outside SkyWest, except when there is a legitimate business reason, and appropriate steps have been taken to assure the information is not misused. If doubt exists as to whether the information is material or has been released to the public, do not trade or discuss it with others until consulting with Investor Relations.

- C. In order to avoid the appearance that any Company employee is trading on inside information, no employee should engage in speculative trading such as short sales or trade in puts, calls, or other options on SkyWest and affiliates stock. Employees may purchase or sell SkyWest securities and exercise options granted to them, as long as they are not basing decisions on inside information.
- D. Stricter standards may apply to officers, directors, and certain other management employees. Management employees should check with their manager or the Director Government and Legal Affairs to determine whether they are subject to this policy. SkyWest's policy regarding communications with the investment community and the proper disclosure of Company information is addressed in detail in [Company Policy Manual SP 158 Corporate Disclosure Policy](#).

8. COMPANY RECORDS

- A. SkyWest's policy requires all accounting reports, financial statements and other business records, document transactions, and events to conform to legal requirements and generally accepted accounting principles as well as to SkyWest's system of internal controls.
- B. Dishonest and unethical reporting within the Company or to organizations or people outside the Company is strictly prohibited. Undisclosed or unrecorded funds or assets are not allowed, unless permitted by applicable law or regulation. All records should be retained and destroyed according to SkyWest's Document Retention Program.

NOTE: Employees are expected to use the Ethics and Grievance Hotline (888.273.9994) to report suspected accounting irregularities and false entries.

9. EMPLOYEE INFORMATION

- A. Records containing any personal information must be kept confidential. Access to such records is limited to managers and others with a specific need to use the information in the performance of their duties.

10. PROTECTION OF COMPANY ASSETS

- A. All SkyWest employees have a special responsibility to protect and ensure the efficient use and care of the Company's physical, financial, and other Company assets. Employees must not use these assets for any purpose not related to Company business without proper authorization. Employees must contact their direct supervisor or manager with any questions regarding this policy.
- B. To ensure the security of both assets and personnel, SkyWest uses video surveillance cameras in various locations. Video recordings may be used by the Company for any purpose, including reviewing injuries, theft, altercations, and other incidents involving passengers or employees. Recorded video media is the property of the Company and may be released to law enforcement at the Company's discretion or by court order.

11. PROTECTION OF INTELLECTUAL PROPERTY

- A. The materials, products, designs, plans, ideas, and data of SkyWest are the property of the employer and should never be given to an outside firm or individual except through normal channels and with appropriate authorization. Any improper transfer of material or disclosure of information is prohibited. Any employee who participates in such a practice is subject to corrective action, up to and including termination of employment. All SkyWest data or intellectual property developed or gained during the period of employment remains the property of SkyWest and must not be retained beyond termination or reused for any other purpose.

NOTE: SkyWest's name, logo, trademarks, and service marks can only be used for authorized Company business and never in conjunction with personal or other activities, unless appropriate approval is received prior to use.

- B. SkyWest's policy is to identify, establish, protect, and defend its rights in all intellectual property assets, including patents, trademarks, copyrights, and other proprietary information. Employees must safeguard these assets and identify and disclose any new works of authorship, technology

advances, and/or unique solutions to business problems to enable SkyWest to establish and protect its rights to such proprietary assets. The intellectual property assets of SkyWest are used for authorized Company business only. In order to respect the valid and legitimate intellectual property rights of others, employees must consult with their supervisor concerning necessary licenses and approvals to use such intellectual property.

12. PROTECTION OF INFORMATION AND DATA SOURCES

- A. Company, employee, partner, and customer information must be protected from unauthorized modification, destruction, loss, and improper disclosure, including partner business plans or strategies, to anyone outside of SkyWest without the authority to do so. Sensitive electronic data must be maintained in secured systems and adequately protected when reproduced on paper. Sensitive documents and reports must be shredded when no longer needed.
- B. Employees must not disclose or reveal any confidential information entrusted to them by the Company, except when disclosure is authorized by the Director Government and Legal Affairs or required by laws or regulation. Confidential information includes all non-public information that might be of use to competitors or harmful to SkyWest or our customers, if disclosed. Examples of confidential information include, but are not limited to the following:
- Detailed financial figures
 - Medical history and drug/alcohol testing results
 - New product or marketing plans
 - Technical information
 - Litigation information
 - Potential acquisitions
 - Divestitures
 - Contracts and alliance agreements
 - Personal information about SkyWest employees and/or customers
- C. No confidential or sensitive Company or employee information should be stored on portable digital storage devices (e.g., portable disk drives, flash drives, CD/DVD-ROM, laptop computers, non-authorized SkyWest equipment) unless properly encrypted. Third party cloud storage services (e.g., iCloud, OneDrive, and Dropbox) should not be used to store confidential or sensitive SkyWest, partner, or employee information.
- D. Data Backup
- 1) The SkyWest IT Department is responsible for maintaining adequate data replication and data backups to prevent the loss of data from accidental deletion or corruption of data, system failure, or disaster. This includes data stored on servers, network attached storage (NAS), and storage area network (SAN) devices.
 - 2) Individuals must ensure that all important information is saved to network data drives rather than local PC and laptop data drives. This will allow IT department backup processes to capture the data.
- E. Working Off-site
- 1) The following controls must be applied when laptops and mobile devices will be taken off-site or used to access confidential and sensitive information:
 - a) Equipment and media must not be left unattended in public places or left in sight in a car.
 - b) Laptops must be carried as hand luggage when travelling.
 - c) Laptops, mobile phones, smartphones, and tablets must be protected at least by a password or a PIN and, where available, encryption.
 - 2) You must immediately notify the IT Department if a device containing PII, financial, confidential, or sensitive data has been lost.
- F. SkyWest computer systems are protected by logon ID and password access restrictions. All user IDs and passwords are to be uniquely assigned to named individuals, and those individuals are accountable for all actions on the IT systems. Any suspected breaches of security or security policy should be reported to your line management or the IT helpdesk as soon as possible.

- 1) System users must maintain confidentiality of passwords and change passwords periodically as prompted by system requirements or SkyWest procedures. Password changes should also occur anytime there is concern a password has been compromised, or inappropriate access to sensitive data is suspected.
 - 2) System users must log off from systems when they are not used or monitored.
 - 3) System users may not perform any unauthorized changes to SkyWest IT systems or information.
 - 4) System users may not attempt to access data that they are not authorized to use or access.
 - 5) System users must not exceed the limits of their authorization or specific business need to access the system or data.
- G. Software may only be installed or upgraded on SkyWest's computer systems by or under the specific direction of SkyWest IT personnel. Under no circumstances should anyone load personal software (any software not purchased/licensed by SkyWest) on SkyWest's computer systems.
- H. The IT Department has implemented centralized, automated virus detection and virus software updates within SkyWest. All PCs have antivirus software installed to prevent and detect viruses and malware. Individuals must not remove or disable anti-virus software.

NOTE: The SkyWest IT Department is responsible for maintaining adequate licensing and ensuring adherence to licensing agreements.

- I. Internet/Intranet access is provided according to management approval. Use of SkyWest internet and email is intended for business use. Access is filtered for SkyWest business purposes and is subject to the following policies:
- 1) Accessing, displaying, or storing any sexually explicit image or document on a Company system is a violation of our Company policy on sexual harassment (refer to [Company Policy Manual SP 53 Productive Work Environment](#)).
 - 2) SkyWest Internet facilities and computing resources must not be used to violate the laws or regulations of any city, state, or nation. This includes adherence to all intellectual property, obscenity, security, and privacy laws.
 - 3) Copyrighted material, files, or programs may not be downloaded from the Internet, unless specifically authorized by IT personnel.
 - 4) Streamlining/downloading items that consume a volume of bandwidth and impact the normal operation of SkyWest Online, SkyTrac, etc. (e.g., Pandora, live tv) is prohibited.
 - 5) SkyWest has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation and to protect against misuse.
- J. Company electronic messaging systems including My Messages, Microsoft Outlook/Exchange, and Microsoft Lync are subject to the following policies:
- 1) Messages and applicable file attachments created, sent, or received via Company email or My Messages are the property of SkyWest. These messages are maintained in Company archive systems for five years and are subject to Company review.
 - 2) Email messages concerning regulatory issues or commercial contracts which require retention longer than five years must be moved to a **Long-term Retention** folder under the Microsoft Outlook mailbox before the two year retention limit is reached. Long-term retention capability must be requested through the IT Department.
 - 3) No email archives should be maintained on portable storage devices.
 - 4) Email messages and signature lines must adhere to the Company branding standards provided in [Company Policy Manual SP 160 Company Identity and Logo Usage](#).
 - 5) Internet-based email systems (Gmail, Hotmail, Yahoo, etc.) should not be used to conduct Company business or to communicate proprietary Company information.
 - 6) Messages sent via Company-provided instant messaging systems are not recorded or archived.

- 7) Use the email systems in a way that could affect its reliability or effectiveness (e.g., distributing chain letters or spam).
- 8) Send unprotected sensitive or confidential information externally.
- K. Voice Equipment Conditions of Use
 - 1) SkyWest voice communication equipment is intended for business use only. Individuals must not use SkyWest long distance or toll-free calling services for personal matters. All Company communication services must never be used to make hoax or threatening calls.
- L. Unauthorized use of audio/video recording devices by employees while on duty, or when in public wearing a SkyWest ID and/or uniform, is prohibited. Company images and information, including aircraft photos and all other operational specifics, cannot be recorded for the purpose of public posting, commercial use, or use in any type of social media (e.g., Twitter, Facebook, email, blogging). The use of any Company images or information for such purposes is strictly prohibited.

13. GIFTS, FAVORS, AND ENTERTAINMENT

- A. SkyWest considers a gift to include any items, products, or services of value given to an employee by an existing or potential competitor, supplier, customer, or other party with whom SkyWest does business. For example, tickets to sporting or other events where the provider has no intention of accompanying the SkyWest recipient are considered gifts. This definition also includes cash in any amount, any items or services purchased at a lower-than-normal price, and any favors, benefits, or other things of value.
- B. Gifts may be offered only if they are modest in value and normal and customary given the business circumstance. Gifts may be solicited for Company-approved business activities or charities only and not for personal use.
- C. No gift may be offered or accepted if a feeling of obligation, a compromise in judgment, or an improper influence on the recipient is created. SkyWest employees may accept nominal gifts but may not accept gifts of cash or cash equivalents (e.g., gift certificates, gift cards). Questions regarding whether or not a gift is inappropriate should be discussed with a supervisor or manager.

NOTE: Departments may choose to establish more restrictive gift and entertainment guidelines than those described above.

- D. Employees who receive gifts that may violate this policy should promptly notify their supervisor, and the gift should be returned with a letter explaining Company policy. When a gift is impractical to return, management may use the gift as a donation to a recognized charity or as a form of employee recognition through the use of a raffle. The gift may not be awarded directly to the recipient.
- E. Items or services customarily provided to Company or travel industry employees (e.g., discounted travel, discounted hotel accommodations) are generally acceptable and are not considered gifts. Discounts on personal purchases are also acceptable, provided such discounts are generally offered to Company employees or others having a similar business relationship with the supplier or customer.
- F. Meals and entertainment that occur in conjunction with business meetings and conferences are a common business practice and do not constitute a gift; however, such occasions should further the business interests of SkyWest and should not be in excess of generally accepted business practices. If in doubt, approval should be obtained from a director or above.
- G. Invitations to business functions that involve customer or supplier-provided overnight accommodations may be accepted only with the prior written approval of a senior officer. While the Company is in the process of sourcing and negotiating supplier contracts, invitations for entertainment (e.g., sporting events, expensive dinners) should not be accepted.

NOTE: Employees must not solicit entertainment from suppliers or customers.

14. SKYWEST AND THE LAW

- A. All SkyWest employees are expected to fully comply with all applicable laws, rules, and regulations anywhere Company business is conducted. Employees may not use a contractor, consultant, agent, or other third party to do anything they themselves are prohibited from doing. Employees must inform a manager, the Ethics and Grievance Hotline (888.273.9994), or the Director Government and Legal Affairs of any violations of laws or regulations.
- B. All employees involved in litigation discovery shall:
 - 1) Treat litigation discovery as a priority.
 - 2) Fully and completely comply with the instructions received from Company attorneys handling the matter.
 - 3) Thoroughly review any questions they have with Company attorneys handling the matter.

15. CORRECTIVE ACTION

- A. Employees who violate SkyWest policy, including this Code, may be subject to corrective action, up to and including termination of employment. Employees who commit criminal acts may be subject to immediate termination and/or possible civil or criminal prosecution. Obstructing or undermining investigations, withholding or destroying information, including failing to report a violation, or providing misleading information are violations of this Code.