

Schiphol Nederland B.V. Code of Conduct

Effective 1 January 2014

Contents

1. General

Article 1 Principles
Article 2 Scope of Code of Conduct
Article 3 General rules of conduct

2. Undesirable behaviour

Article 1 Undesirable behaviour
Article 2 Reporting undesirable behaviour

3. Business relations

Article 1 General principle: be loyal to the company
Article 2 Value of business gifts
Article 3 Business visits
Article 4 Responsible business conduct
Article 5 Fair competition and the fair treatment of business relations and suppliers

4. Use of the available ICT resources

Article 1 General principles
Article 2 User names and passwords
Article 3 The Internet
Article 4 E-mail
Article 5 Use of a smartphone or tablet
Article 6 Checks

5. Fraud

Article 1 Report all types of fraud
Article 2 Reporting

6. Reporting abuse

Article 1 Abuse
Article 2 Procedure

7. Internal reporting procedure

Article 1 Scope and objective
Article 2 Reporting
Article 3 Procedure
Article 4 Alternative procedure
Article 5 Protection of the informant
Article 6 Protection of the accused
Article 7 Data protection and privacy

Use your common sense

1. General

Article 1 Principles

1. Schiphol Nederland B.V. (hereinafter referred to as SNBV) conducts its operations with due regard for integrity, transparency and accountability. These principles constitute the basis of the Code of Conduct applicable to SNBV. The Code of Conduct contains provisions relating to the following:

- a. undesirable behaviour
- b. the manner in which employees should deal with business relations
- c. the manner in which employees should use the available ICT resources
- d. fraud and other types of abuse

2. The Code of Conduct is based on an active and passive approach. This means that employees are not only deemed to comply with the Code of Conduct but that they are, in turn, deemed to report any suspected conduct that violates the Code.

3. SNBV monitors whether employees comply with the Code of Conduct. If they violate the Code of Conduct, SNBV may impose disciplinary measures.

4. All employees must report any suspected violations of the Code of Conduct to their manager or immediate senior manager. The confidential adviser acts as a sounding board for employees intending to report improper conduct. Employees may also use the anonymous Integrity Reporting Line if it is not possible or advisable to report improper conduct to the manager (or the manager's supervisor) for any reason. See §7 of the Code of Code for further information on the reporting procedure.

Article 2 Scope of Code of Conduct

The Code of Conduct applies to all individuals with an SNBV employment contract. The Code of Conduct equally applies to individuals who perform services for SNBV as a contractor. It furthermore applies to all other users of SNBV's computer network and external connections. A user means any person who has been given access to the SNBV computer network on the instructions of SNBV. Where relevant, the Code of Conduct also applies to employees whose employment contract has been terminated.

Article 3 General rules of conduct

1. In general in the performance of their duties employees are expected to act in the interests of SNBV at all times. This means that employees (whether or not acting in the name of SNBV) must comply with all the applicable laws and regulations, including anti-discrimination, competition, public procurement, privacy, fraud, anti-corruption and bribery laws. Employees must furthermore adhere to the internal regulations and procedures.

2. Managers serve as role models for their subordinates. Therefore they themselves must not only act in accordance with the Code of Conduct but they moreover fulfil a supervisory, signalling and corrective role.

3. At Schiphol it is compulsory to present proof of one's identity. A Schiphol Pass is a personal identity document and provides access to the security-restricted areas. It is important to use the pass with the utmost care. A Schiphol Pass must always be worn visibly in the security-restricted areas.

4. Press Relations and Corporate Affairs (D/CA) is the only department that may act as the spokesperson on Schiphol matters. If a journalist approaches an employee for information or if an employee is invited to speak or hold a presentation for or on behalf of the company, it is important that the employee obtains prior consent from D/CA accordingly.

5. When processing personal data employees must act in accordance with the applicable privacy regulations. The reports made by SNBV on the basis of the Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*) are administered by the SNBV Data Protection Officer.

6. Employees must administer documents and data files with due care in accordance with the applicable procedures and guidelines.

Act with respect

2. Undesirable behaviour

Article 1 Undesirable behaviour

Employees must refrain from displaying any type of behaviour that may be deemed undesirable. Within the meaning of this section, undesirable behaviour means approaching a person in an undesirable manner which the person concerned finds threatening, humiliating or intimidating. This in any case refers to the following situations:

- a. **Sexual harassment:** Behaviour of a sexual in nature which the employee finds unwelcome or threatening and could damage the working relationship.
- b. **Aggression and violence:** psychologically or physically harassing, threatening or assaulting a person at work or in connection with work.
- c. **Discrimination:** the prejudicial treatment of groups or individuals based on religion, belief, political affinity, race, gender, nationality, sexual orientation, marital status, or on any other grounds.
- d. **Bullying:** the systematic inflicting of hurt on and/or the harassing of an employee by one or more employees.

Article 2 Reporting undesirable behaviour

Employees who find certain types of behaviour undesirable may report this to their manager or immediate senior manager. Should this not be possible or advisable, the employee may use the anonymous Integrity Reporting Line. The course of the reporting procedure is explained in the internal reporting procedure under §7 of this Code of Code. The confidential adviser acts as a sounding board for employees intending to report undesirable behaviour.

Even the semblance of susceptibility to influence must be avoided

3. Business relations

Article 1 General principle: be loyal to the company

1. In maintaining contact with business relations the interests of SNBV serve as the guiding principle.
2. Every employee must avoid a seemingly dependent position by mixing business with private interests. Private interests are also taken to mean the interests of partners, blood relatives and relatives by marriage up to the fourth degree. In the event of doubt concerning a possible conflict of interest, the employee must take the initiative to notify his or her manager as soon as possible.
3. Employees may not ask for or accept any cash or cash equivalents from current or prospective business relations. They may furthermore not accept any gifts, entertainment, favours or services insofar as they fall outside the scope of this regulation. Even the semblance of susceptibility to influence must be avoided
4. Employees working for the Schiphol Real Estate business area may furthermore not conduct any real estate transactions for their own account without the consent of the director of Schiphol Real Estate, such as acquiring, developing, disposing of or participating in real estate or real estate securities. The above prohibition self-evidently does not apply to standard transactions, such as buying a house. This provision applies equally to employees who do not work for Schiphol Real Estate but who, by virtue of their position have knowledge of, or are involved in specific real estate-related issues.

Article 2 Scope of business gift policy

1. In general employees must avoid being offered business gifts as far as possible. Nonetheless if an employee is offered a business gift, the rule is that the employee may accept a business gift having a maximum retail value of EUR 100 once a year per supplier. Furthermore the employee who takes receipt of the business gift must clearly have a business relationship with the supplier. If employees are offered a business gift in contravention of the provisions of this article they must report this to their manager.
2. When giving business gifts employees must act in the spirit of this Code of Conduct.

Article 3 Business visits

Employees whose work involves visiting clients and/or suppliers must always submit any expense claims for such visits to SNBV.

Article 4 Responsible business conduct

1. In conducting business responsibly the following should be taken into account:
 - choose reliable partners (business relations, suppliers and service providers);
 - do not grant these partners any private transactions;
 - set out material arrangements, agreements and contracts in writing;
 - freeze relations temporarily if a partner intentionally violates the law or a substantial SNBV rule of conduct and consult senior management about possibly terminating the business relationship;
 - ensure that all the amounts paid by SNBV either directly or indirectly, both now or later, in connection with a supplier's order, are in fact credited to the supplier and no one else.
 - ensure that no business is conducted in or with countries against which international sanctions have been proclaimed.
2. The following rules apply to attending events (such as a soccer match, golf events, business anniversaries, theatre performances and exhibitions) on the invitation of clients or suppliers:
 - Employees must immediately notify their manager that they have been invited by a party to an event.
 - The manager will decide in consultation with the employee concerned whether s/he may accept the invitation, any conditions that may be attached and how the party issuing the invitation will be notified accordingly.
 - Any travel and accommodation costs attached to the event will be borne by the relevant employee.

Article 5 Fair competition and the fair treatment of business relations and suppliers

1. Relevant business relations and suppliers must have an equal opportunity to compete for contracts.
2. Prospective business relations and suppliers must be given the same level of information.
3. The information provided to business relations and suppliers must be correct, neutral and not misleading.
4. The responsible procurement officer and/or jurist must always be involved in good time.

Handle with care and prevent misuse

4. Use of the available ICT resources

Article 1 General principles

1. All ICT resources made available are primarily intended for business use and must be used with due care at all times. The ICT resources referred to in this section mean all resources made available for exchanging information electronically, such as computers, tablets and smartphones and the accompanying software, as well as the Internet, e-mail and Wi-Fi connections.

2. The following general rules must be observed:

- SNBV's business has priority and may under no circumstances be jeopardised either directly or indirectly. Users of ICT resources (hereinafter referred to as the 'User') must be aware that all their actions can be traced back directly to SNBV and they must act in the appropriate manner.
- Employees are not permitted to develop activities that may tarnish SNBV's good reputation.
- The loss or theft of ICT resources must be reported to the ICT Service Desk as soon as reasonably possible.
- The use of ICT resources with the aid of notebooks, tablets, and similar equipment (whether or not privately owned or brought along by employees) is only permitted on the wireless or non-wireless network connections made available for that purpose.
- ICT resources that have not been used for a period exceeding 90 days will automatically be cancelled or withdrawn, unless other specific arrangements have been made.

All ICT resources made available are and remain the property of SNBV. On leaving employment or when the activities have ended, the User must hand in all ICT resources made available to the ICT service desk.

Article 2 User names and passwords

1. The user names and passwords to be used for the various ICT resources must be used with due care. Passwords must be chosen carefully and should at least be composed of both letters and numerals, include one capital letter.

Article 3 Internet

1. Users may use the Internet to a limited extent for non-business purposes, provided that this does not disrupt day-to-day activities.

2. The Internet may never be used for the following purposes:

- Visiting or viewing sites containing pornographic, discriminatory, insulting or offensive material and downloading material from these sites. Users must notify their manager if they are offered material of this nature unsolicited.
- Gambling or taking part in games of chance.

3. Users may not use social media without prior consent for the following purposes:

- Posting information about SNBV.
- Responding to online statements concerning SNBV or the airport on their own initiative.
- Sharing other information known to Users by virtue of their position.

Article 4 E-mail

1. Users may correspond by e-mail to a limited extent for non-business purposes, provided that this does not disrupt day-to-day activities.

2. E-mail may never be used for the following purposes:

- Discrediting the SNBV organisation.
- Sending anonymous messages under a fictitious name.
- Sending confidential documents unprotected by e-mail to an external address.
- Sending or forwarding threatening, insulting, sexually-oriented, racist or discriminatory messages and chain letters. Users must notify their manager if they are offered material of this nature unsolicited.
- Harassing a person.

3. The employer or the company investigation service may access an employee's mailbox provided there is a business reason for doing so and proportionate action is taken

Article 5 Use of a smartphone or tablet

1. Smartphone or tablet users must use the equipment with due care. 'Use with due care' refers not only to the smartphone or tablet itself but also to using the business information or other information accessible via a smartphone or tablet with due care.
2. All reasonable smartphone or tablet usage costs will, in principle, be borne by SNBV. However, a number of conditions and restrictions apply:
 - A monthly maximum data usage cap of 500 MB.
 - Calling 0900 numbers, other than for business purposes is not permitted.
 - The use of SMS payment or other services and/or taking part in telephone games and suchlike is not permitted.
 - Any costs incurred outside the Netherlands should be for business purposes only. Users must be aware that telephone and data usage outside the Netherlands (including data streaming, the use of navigation software and sending photographs and files) can be very costly. Users must therefore keep telephone calls they make abroad or to other countries as short as possible and use any Wi-Fi networks as much as possible.
3. All costs arising from misuse, negligent use or costs otherwise arising from use that conflicts with the conditions imposed may be charged to the User and/or set off against the User's salary. If misuse or serious negligence has actually taken place, SNBV may moreover take appropriate disciplinary or other measures.

Article 6 Checks

1. SNBV may carry out checks to ensure the security of the network and to monitor careful use in accordance with this section. Use of the Internet and e-mail communications may be investigated at random by, for instance, examining the time spent and the sites visited. Anonymous lists of the Internet sites visited and the e-mails sent may be printed for the purpose of the investigation.
2. Incoming Internet and e-mail communications will be monitored for viruses and spam. Should a virus be found in an e-mail message, the message will usually be blocked automatically and the sender and recipient will be notified accordingly. Users must promptly contact the ICT Service Desk, extension 4445, if they nevertheless receive an e-mail message that might contain a virus.
3. If a person is suspected of violating these rules, the information relating to the User(s) concerned may be printed, examined and used by the company investigation service. The Director of Human Resources will receive prior notification of any such investigation by the company investigation service.
4. Personal data will only be retained if there is a serious suspicion that the rules have been violated. In other cases the information that can be traced back to individuals will be destroyed immediately.
5. The information will be retained until such time as the investigation has been finalised and any measures taken.

Reporting fraud

5. Fraud

Article 1 Report all types of fraud

Within the meaning of this section, fraud is defined as all unauthorised, irregularities caused intentionally with material or immaterial gains in mind on the part of the fraudster or a party/parties known to the fraudster, due to which SNBV and/or the employee(s) concerned suffer or may suffer damage or a loss.

Article 2 Reporting

Every employee or third party must avoid any suspicion of fraud. Employees must report such suspicions to their manager or immediate senior manager. Should this not be possible or advisable, the employee must use the anonymous Integrity Reporting Line to report suspected fraud. The course of the reporting procedure is explained in the internal reporting procedure under §7 of this Code of Code. The confidential adviser acts as a sounding board for employees intending to report suspected fraud.

Report suspected abuse

6. Reporting abuse

Article 1 Abuse

1. Every employee must report any negligent, unethical or improper acts or any other form of suspected abuse. Suspected abuse is taken to mean a suspicion based on reasonable grounds that the following is taking place at SNBV:
- a. an actual or impending criminal act;
 - b. an actual or impending violation of laws and regulations;
 - c. a risk to public health, security or the environment;
 - d. actually informing or threatening to deliberately inform public bodies incorrectly;
 - e. a violation of the company Code of Conduct;
 - f. actually or threatening to deliberately withhold, destroy or manipulate information about such facts.

Article 2 Procedure

Employees must notify their manager or immediate senior manager of suspected abuse. Should this not be possible or advisable, the employee must use the anonymous Integrity Reporting Line to report suspected abuse. The course of the reporting procedure is explained in the internal reporting procedure under §7 of this Code of Code. The confidential adviser acts as a sounding board for employees intending to report suspected abuse.

The reporting procedure

7. Internal reporting procedure

Article 1 Scope and objective

The internal reporting procedure describes the procedure for reporting any fraudulent, unethical or unlawful conduct and conduct that violates the Code of Conduct

Article 2 Reporting

1. Employees are deemed to report improper conduct to their manager or immediate senior manager. The confidential adviser acts as a sounding board for employees intending to report improper conduct. If employees wish to remain anonymous, they should use the anonymous Integrity Reporting Line. Further details of how the Integrity Reporting Line works can be found on the intranet.
2. To minimise obscure and false reports, anonymous reports, received through channels other than the Integrity Reporting Line, will not be examined. It should be clear that making a false report will not be tolerated under any circumstances. Making a false report is deemed a serious violation of the Code of Conduct.

Article 3 Procedure

1. The manager forwards every report received to the Integrity Committee, which can be reached through: integriteitscommissie@schiphol.nl. The committee consists of the Chief Financial Officer, the Director of Corporate Legal, the Director of Corporate Audit Services, the Director of Human Resources, the Director of Safety, Security & the Environment and the Works Council Chair. Reports received through the Integrity Reporting Line are forwarded to the Integrity Committee anonymously.
2. On receipt of a report, the Integrity Committee evaluates and assesses the report and determines the action to be taken. If desired, the Integrity Committee may ask for additional information. If a report was made anonymously, additional information may be obtained anonymously through the Integrity Reporting Line.

Integrity Reporting Line (anonymous)

Manager or his/her manager (possibly the confidential adviser as the sounding board).

Report

Integrity Committee

Investigation and/or action

3. As soon as sufficient clarity has been obtained on the report, the Integrity Committee may decide to conduct a further investigation. The Integrity Committee may also decide to examine the report itself or may request the person/department/committee having the most expertise to further examine the report.
4. The Integrity Committee ensures that every report is handled in the proper manner, is documented correctly and where necessary reported in the appropriate manner to the responsible bodies. Where reasonably possible, the informant will be periodically kept informed of progress.
5. The Integrity Committee reports to the Supervisory Board Audit Committee, the Management Board and the external auditor annually.
6. The Integrity Committee treats all the information obtained as confidential. Employees and/or third parties will not be given any information without the consent of the Integrity Committee. The informant's anonymity will be protected if the information is required for legal or judicial reasons.

Article 4 Alternative procedure

1. In the event the report concerns or relates directly to a Management Board member or a member of the Integrity Committee, or if it is inadvisable to make a report to the Integrity Committee for another compelling reason, an alternative procedure applies.
2. In this case the manager forwards the report to the Corporate Secretary. If a report is made through the Integrity Reporting Line, the person can use a different access code to ensure that the report reaches the Corporate Secretary. Further information about the reporting procedure is available on the intranet.

3. If the report concerns or relates directly to a member of the Management Board, the Corporate Secretary subsequently forwards the report to the Supervisory Board Chairman. In all other cases the Corporate Secretary forwards the report to the President & CEO.

4. The President & CEO or the Supervisory Board Chairman will then handle the report in the appropriate manner. The procedure followed is similar to that set out in Article 3 of these regulations.

Integrity Reporting Line (anonymous)

The report concerns a member of the Integrity Committee

Corporate Secretary

Investigation and/or action by the President & CEO of the Management Board

Integrity Reporting Line (anonymous)

The report concerns a Management Board member

Corporate Secretary

Investigation and/or action by the Supervisory Board Chairman

Manager or his/her manager (possibly the confidential adviser as the sounding board).

Manager or his/her manager (possibly the confidential adviser as the sounding board).

Article 5 Protection of the informant

1. The identity of the informant will be protected and the latter will be protected from retaliatory measures by SNBV, subject to the exceptions stated in paragraph 2.

2. There are three exceptions on the basis of which the informant will not enjoy protection. This applies if:

- a. The informant does not abide by the internal procedure.
- b. The report concerns malicious intent.
- c. The report itself is a serious violation or a crime.

3. If the informant is dissatisfied with the way the report was handled or with the outcome, feels threatened or is having to contend with retaliatory measures, s/he may submit a complaint directly to the person or committee who initially was notified of the report. The complaint may of course also be reported through the Integrity Reporting Line.

Article 6 Protection of the accused

1. If an official investigation is to be conducted into a person, the employer will, in principle, notify the person who is to undergo investigation within three days. The period may be extended if there is a risk that evidence will be destroyed and/or the investigation obstructed.

2. The person under investigation is entitled to lodge an appeal against the fact that s/he is subject to an investigation with the Board of Appeal.

Article 7 Data protection and privacy

1. The Integrity Committee and the designated executives will treat all the information received as strictly confidential. The privacy of both the informant and the accused will be protected.