SMC® Ltd.

Global Privacy Policy

For all SMC employees, job applicants and agency staff working for SMC Ltd.

Purpose

The purpose of this Policy is to ensure compliance to global information privacy laws by all employees, job applicants and agency staff working for SMC Ltd. (SMC). SMC is committed to treating personal information confidentially through compliance with relevant local, state and country laws within sound operational and technology standards.

This policy addresses how personal information is secured and handled within SMC and is not intended to contain the details of every procedure, but instead provides a framework for processing personal information.

Definitions

Personal Information (also referred to as personal data):

a. This includes any information about a current, past or temporary employee, including dependents;
b. Information kept on paper or electronically;
c. Any information. from which a person can be directly or indirectly identified.

Examples of personal information include: a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Sensitive personal data: Includes, but is not limited to, information such as: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, information concerning health, or sexual orientation.

SMC Devices: Devices include, but are not limited to computer hardware, software, Internet / Intranet access, email, storage, applications, instant / text messaging, mobile devices (smartphone, cell phone or tablet) and any other hardware or software, managed or controlled by SMC.

Children's Privacy

A child is considered to be anyone under the age of 16, and in some countries 13 years old. SMC does not routinely process information about children but where we may hold that information, such as benefits, including, life, dental or medical insurance, explicit consent from those with legal guardianship will take place.

Accountability

SMC allows employees to access personal data with the mutual understanding they handle information confidentially and exercise good judgement. All information should be created, stored and accessed in a manner consistent with this policy and / or applicable laws. (See Section User Responsibilities).

a. Leaders
   Formal Leaders are responsible for ensuring this privacy policy is followed and the mandatory Data Protection Awareness training is completed. (See Section Learning and Development).
b. Data Security Coordinator
   - Oversees compliance with this policy Company-wide;
   - Serves as nominated initial point of contact for SMC;
   - Understands the primary systems, processes and controls that support compliance to this policy;
   - Keeps up-to-date with local privacy laws and regulations, and confirms the appropriateness and applicability to local Global Privacy material;
   - Reviews material as necessary to ensure local compliance and implementation;
   - Manages issues about personal information from data subjects;
   - Manages personal information breaches.

Information We Collect

We collect employee information from prospective and present employees for legitimate business purposes. Primarily, this information is used for the purpose of payroll, but can be requested for other purposes including, but not limited to business travel, health insurance, and other benefits administration. Employee information on health, performance evaluations, and other sensitive employee matters, whether it is stored physically or electronically, is accessible by appropriate employees only if necessary with respect to a legitimate business need. Employee pictures and employee information may be shared internally, however, any use for external purposes will be shared only after receiving written authorization by the employee.

For legitimate Human Resources purposes, employees may choose to voluntarily disclose personal data about family members. If an employee chooses to disclose this information, their family members' personal data shall be treated, for the purposes of this policy, the same as an employee's personal data. Employee information is never sold, leased, or rented to a third party. Employee information is not disclosed to third parties except as follows:

a. To those retained by us for processing only for the purposes set forth in this policy;
b. Where required pursuant to an applicable law, governmental or judicial order, or to protect Company rights or property;
c. Where authorized electronically or in writing by the employee;
d. Where the employee voluntarily provides personal data and the context makes it clear that employee information will be provided to a third party / subprocessor.

How We Store Personal Data

All data provided is stored on secure servers; the transmission of information via the Internet is never completely secure. Although we will do our best to protect personal data, we cannot guarantee the security of data transmitted to our site or any of our partner sites. SMC will use strict procedures and security features to protect any personal data received.

Retention of Personal Data

SMC will retain personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required to be kept by law.

Rights

SMC will ensure all employees are aware of their data protection rights. Every user is entitled to the following:

a. The right to know what personal information is collected, used, or shared;
b. The right to access and / or request copies of personal data from SMC, for which a small fee may be charged;
c. The right to rectification requesting SMC corrects any inaccurate or incomplete information;
d. The right to erasure requesting SMC or any of its service providers erase personal data under certain conditions;
e. The right to restrict processing of personal data, under certain conditions;
f. The right to object to processing of personal data, under certain conditions;

g. The right to data portability requesting SMC transfer the data collected to another organization, or directly to data subject, under certain conditions;
h. The right to non-discrimination in terms of price or service when an employee exercises a privacy right under the applicable law.

Privacy Shield Frameworks for European Union (EU) and Swiss Citizens

SMC complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries (including Iceland, Liechtenstein, and Norway) and Switzerland transferred to the United States pursuant to Privacy Shield. SMC has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this privacy policy and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit: https://www.privacyshield.gov/.

User Responsibilities

Users of SMC devices agree to not:

a. Alter or change files or systems without authorization;
b. Hack into internal or external SMC systems or informational databases;
c. Scan networks for security vulnerabilities without authorization;
d. Alter any SMC computing or networking components (including, but not limited to bridges, routers, switches and hubs) without authorization;
e. Create unauthorized network connections, including unauthorized extensions or re-transmission of any computer or network services;
f. Intentionally damage or destroy the integrity of electronic information or intentionally disrupt the use of electronic networks or information systems;
g. Access, create or share illegal material including websites relating to terrorism, illegal weapons, illegal or malicious websites providing network or computer hacking content, websites instructing how to commit or enable any form of fraud, gambling or piracy of copywritten material such as software, film, or music;
h. Access, create or share obscene or pornographic material, or any other material that may be considered offensive or in bad taste;
i. Store SMC information in any personal file sharing applications that have not been approved by SMC, or disclose material in the public domain that should be kept inside of SMC, e.g. by publishing the information on a website or presentation software, or placing information that should not

be shared in applications where others will be able to access it unless authorized to do so;

j. Copy or use licensed computer software without the permission of SMC IT;
k. Download, send or store any non-SMC supplied software, such as unauthorized names, web browser plug-ins, instant messaging (e.g. Yahoo Messenger), peer-to-peer file sharing (e.g. open source, public-domain software or freeware) without prior approval from SMC IT. SMC reserves the right to remove any unauthorized or illegal software from SMC IT devices without notice to the user;
l. Use Webmail (e.g. Gmail, Hotmail, Yahoo mail) for business purposes.

Copyright Material

Information available on the Internet may not be freely available for sharing, downloading or printing. Check copyright notices and adhere to those requirements for use as generally displayed on the website before reproduction (printing, downloading or copying).

Access to Websites That are Blocked

SMC has Internet content filtering software in place to block access to sites that we classify as inappropriate or a potential threat. If you have a business need to access a website that is blocked, contact the IT Help Desk.

Email and Other Electronic Communications

Employees are provided with and permitted to use email and instant messaging to communicate effectively with other employees and relevant third parties, such as customers, suppliers, and outside consultants so we can efficiently provide our services. All communications sent or received using SMC systems remain the property of SMC and personal use must be in line with this policy and other SMC policies.

When using SMC email or other Company electronic communication systems, employees must ensure that communications are carefully worded and void of using unprofessional or casual comments that could lead to contractual or other legal issues. Employees should also take reasonable steps to prevent unauthorized use of their email account by anyone else, especially by persons not employed by SMC. Please report any suspicious email activity to the IT Help Desk.

Prohibited Email Activity Includes:

a. Interfering with the SMC email system and / or seeking to gain unauthorized access to other employees' email accounts;

b. Alteration of the content of a message originating from another person or computer with the intent to deceive;
c. Using an email address not authorized by SMC for work-related purposes;
d. Using SMC email accounts for personal or political activity, profit or gain;
e. Issuing, forwarding, or responding to chain or gambling emails;
f. Forging, misrepresenting, obscuring, replacing or suppressing a user identity on any electronic communication to mislead the recipient about the sender;
g. Opening attachments from unknown and dubious sources or failing to alert the IT Help Desk of such emails;
h. Forwarding emails containing confidential SMC information and / or attached files or emails that should be kept internal.

Privacy and Monitoring

SMC does not guarantee the confidentiality or privacy of any email, attachment, or instant message sent either internally or externally. SMC may routinely scan, inspect, copy, store and disclose the contents of any email, attachment, or instant message where we are able to do so lawfully and we have reasonable suspicion of non-compliance to the requirements of this policy; these requests will be authorized by members of the Corporate HR and / or Legal teams.

Access to your email or document folders may be given to your Leader or your Human Resources Leader, under the following circumstances:

a. If you are absent from work and it is necessary for legitimate work purposes;
b. Where we have reasonable grounds to suspect non-compliance to this policy;
c. When we are required and permitted to do so by law.

Personal Use of the Internet and Email

Employees can use email and the Internet for personal use when:

a. In compliance with other local and national laws;
b. Consistent with the requirements of this policy;
c. Kept to a reasonable level and
d. It does not prevent an employee from completing his / her job requirements.

SMC accepts no liability in relation to employees' personal use of email and the Internet and any subsequent loss or harm to the employee. Employees with questions regarding Internet usage, should contact their direct Leader.

Mobile Devices

SMC will allow access to Company information on a mobile device for legitimate business purposes only.

a. The device must be registered with SMC IT so a mobile device management system can be uploaded;
b. Users should not allow anyone else to access SMC's information on or from the mobile device;
c. Information should not be transferred outside of the SMC computing environment;
d. Global positioning information is not collected or used by SMC if you have a SMC provided device. If you choose to use this function on any device, you may disclose your personal information including your location to the service provided. SMC is not responsible for any loss or harm as a result.

Password Standards

When choosing passwords, follow these guidelines:

a. Do not use passwords that can be easily guessed, such as family names;
b. Update passwords regularly and do not share passwords with anyone;
c. Do not write passwords down or keep them where easily found;
d. If sending a password protected document, provide the password separately;
e. Do not reveal or use the passwords of others.

Images or Quotations of Employees, Third Parties, Premises or Yourself

Do not capture, store or use any image (picture, video, personal quotation) by any means that identifies an individual unless you have:

a. Gained his / her explicit consent, and
b. A legitimate business purpose.

Do not take or upload images of SMC or customer internal facilities and / or products unless you have gained formal consent and it is relevant to an SMC business objective.

Non-compliance with this Policy

In the event of activity in violation of this policy, employees may be subject to removal of their Internet access and disciplinary action up to and including termination of employment.

Data Protection Breaches and Reporting

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal information transmitted, stored or otherwise processed.

In the event of a personal information breach or suspicion of a breach, employees should immediately notify their Data Security Coordinator or direct Leader. Additionally:

a. If the breach occurs or is discovered outside of normal business hours, notification and any remedial actions should begin as soon as possible;
b. If the breach involves passcodes to the building, the direct Leader should be notified immediately;
c. If the breach involves building access such as loss of a badge, the employee should contact Human Resources immediately. The badge will be inactivated and a new one issued;
d. If the breach relates to the loss of electronic equipment e.g. laptop or memory stick, immediately notify the IT Help Desk.

Learning and Development

We are committed to provide everyone with the skills and ability to demonstrate competence in their role. We do this by:

a. Providing all new, existing, and temporary employees, with data protection training which includes a test of understanding and a 'statement of compliance' consent;
b. Providing regular recurrent training to ensure ongoing support and understanding of this policy.

Policy Communication

This policy is effective immediately. Any changes will be communicated globally via email and SharePoint. All policy and training materials are owned by SMC and will be reviewed annually. Additional reviews may be triggered by changes in strategy or the regulatory environment.

Responsibility

The Vice President Human Resources is responsible for the interpretation of this policy.