NORDIQ CANADA
DEVICE ACCEPTABLE USE POLICY

Definitions

1. Terms in this Policy are defined as follows:
    a) ***Corporate Device –*** A laptop, computer, phone or other device owned or leased by Nordiq Canada and used by Representatives to access Nordiq Canada's network and/or Confidential Information
    b) ***Device*** – Personal Devices and Corporate Devices
    c) ***Confidential Information*** – Personal information of Participants including but not limited to home address, email address, personal phone numbers, date of birth, financial information, medical information, and background check information. Additionally, *Confidential Information* also includes information considered to be intellectual property of Nordiq Canada such as data, proprietary information, business information, and trade secrets
    d) ***Participants*** – Refers to all categories of individual members and/or registrants defined in the By-laws of Nordiq Canada who are subject to the Universal Code of Conduct to Address and Prevent Maltreatment in Sport ("UCCMS") and the policies of Nordiq Canada, as well as all people employed by, contracted by, or engaged in activities with, Nordiq Canada including, but not limited to, employees, contractors, Athletes, coaches, instructors, officials, volunteers, managers, administrators, committee members, parents or guardians, spectators, and Directors and Officers
    e) ***Personal Device*** – A Representative's personal laptop, computer, phone or other device that is being used to access Nordiq Canada's network and/or Confidential Information
    f) ***Representative*** – All individuals employed by, or engaged in activities on behalf of, Nordiq Canada. Representatives include, but are not limited to, staff, administrators, Directors and Officers of Nordiq Canada, committee members, and volunteers

Purpose

2. This Policy defines standards, procedures, and restrictions for Representatives with legitimate business uses connecting Devices to Nordiq Canada's corporate network and/or using Nordiq Canada's digital resources and/or data.

3. The primary goal of this Policy is to protect the integrity of Confidential Information that resides within Nordiq Canada's technology infrastructure, including internal and external cloud services. This Policy intends to prevent Confidential Information from being deliberately or inadvertently stored insecurely on a Device or carried over an insecure network where it could potentially be accessed by unauthorized persons. A breach of this type may result in loss of information, damage to critical applications, loss of revenue, damage to Nordiq Canada's public image, a breach of data privacy requirements, and/or a violation of data privacy laws.

Application

4. This Policy applies to, but is not limited to, all Devices and accompanying media that fit the following classifications:
    a) Smartphones
    b) Other mobile/cellular phones
    c) Tablets
    d) Laptop/notebook computers
    e) Wearable computing devices
    f) Any other mobile device capable of storing corporate data and connecting to a network

5. This Policy applies to any Device that is used to access corporate resources, whether the Device is owned by

the Representative (Personal Device) or by Nordiq Canada (Corporate Device).

Appropriate Use

6. It is the responsibility of any Representative using a Device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied. It is imperative that any Device that is used to conduct Nordiq Canada business be used appropriately, responsibly, and ethically.

Corporate Devices

7. From time to time, Nordiq Canada may permit Representatives to access the Nordiq Canada network and/or Confidential Information on Corporate Devices. Use of Corporate Devices is subject to the following:
    a) All data stored on Corporate Devices is the property of Nordiq Canada
    b) Nordiq Canada has the right to access, inspect, remove or alter all data stored on Corporate Devices at any time and without prior notice
    c) Nordiq Canada has the right to monitor any or all aspects of Corporate Devices including, but not limited to, monitoring sites visited by Representatives on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by Representatives, and reviewing email sent and received by Representatives. Representatives understand that Nordiq Canada may use automated software to monitor material created, stored, sent, or received on its Corporate Devices
    d) The use of passwords to gain access to a Corporate Device or to encode particular files or messages does not imply that Representatives should have an expectation of privacy in the material they create, store, send or receive on a Corporate Device
    e) Representatives may not move or copy programs or any form of Confidential Information or system software from one Corporate Device to another without prior authorization from the Representative's supervisor
    f) Representatives may not download any applications or software onto a Corporate Device without permission from Nordiq Canada

8. Corporate Devices are the property of Nordiq Canada and may only be used for purposes approved by Nordiq Canada. Representatives shall only use computer resources in a professional, ethical and lawful manner.

9. Personal use of Corporate Devices is permitted provided that such use:
    a) Complies with this Policy and every other Policy of Nordiq Canada including but not limited to the *Code of Conduct and Ethics*, *Confidentiality Policy*, and *Social Media Policy*
    b) Does not interfere with performance of their Nordiq Canada-related duties;
    c) Does not negatively impact on the performance or operation of Nordiq Canada computer systems or other Corporate Devices; and
    d) Does not incur cost to Nordiq Canada.

Personal Devices

10. From time to time, Nordiq Canada may permit Representatives to access the Nordiq Canada network and/or Confidential Information on the Representative's own Personal Device. Use of Personal Devices to access the Nordiq Canada network and/or Confidential Information is subject to the following:
    a) Confidential Information or other information or intellectual property that is propriety to Nordiq Canada that is created or modified by a Representative on a Personal Device is owned by Nordiq Canada and, even when stored on a Personal Device, may be accessed by Nordiq Canada in some circumstances including for record retention, investigations, or as a result of litigation
    b) Representatives accessing Nordiq Canada's network and/or Confidential Information on their Personal Device may not save their Nordiq Canada user credentials (such as a login name and

password) to their Personal Device

c) Representatives will delete all Confidential Information from their Personal Device at Nordiq Canada's request and the Representative may be asked to demonstrate to Nordiq Canada that such Confidential Information has been completely removed from the Personal Device
d) In the event the Personal Device is lost or stolen, the Representative must report the incident to Nordiq Canada and describe, in writing, all of the Confidential Information that was stored on the device or otherwise accessible
e) Personal Devices may only be accessed by the Representative. Family or friends of the Representative may not have access to the Personal Device

11. Under no circumstances will Nordiq Canada pay for or reimburse a Representative for using their own Personal Device for any reason including, but not limited to, accessing Nordiq Canada's network or completing work or tasks for Nordiq Canada. The monthly phone allowance provided by Nordiq Canada is to be used to purchase a Corporate Device, which may be used for personal use subject to this policy.

Security

12. Representatives using Devices and related software to use or access Confidential Information will, without exception, use secure data management procedures. Representatives are also expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.

13. All Devices accessing the Nordiq Canada computer network and/or Confidential Information require adequate antivirus protection. Should Nordiq Canada find a Device that is accessing Nordiq Canada computer network and/or Confidential Information without adequate virus protection (adequacy determined pursuant to Nordiq Canada at its sole discretion), Nordiq Canada has the right to refuse service and/or restrict access until such time adequate antivirus protection is installed on the Device.

Policy Non-Compliance

14. Failure to comply with this Policy may, at the discretion of Nordiq Canada, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment (when applicable).