



# Bukhatir Group Policy and Procedure

## Bukhatir-IT Department

# Acceptable Use Policy

Document No: Version 1

Copyright © 2021 Bukhatir Group

This document is the property of **Bukhatir Group**, UAE.

All rights are reserved. No revision of this document can be made, reproduced, distributed or transmitted in any form or by any means, including and not limited to, photocopying, recording or any other electronic means without prior written consent of the **Bukhatir** management.



<b>Name:</b> Acceptable Use	<b>Document Number:</b> BIL - IT - POL-005
<b>Department:</b> Bukhatir-IT	<b>Version Number:</b> 01
<b>Revision Date:</b> 8/March/2021	<b>Effective Date:</b> 9/March/2021

## REVISION CONTROL

This document is issued under the authority of the company and applies when carrying out the activities described. Revisions may be issued, when necessary, under the authority of Bukhatir Group. Revision history and details are required to be recorded below with every revised policy.

## REVISION HISTORY

Ver. No.	Effective Date	Description
1	9/March/2021	Version 1 revised and released for end user sign-off

## REVISION SIGN OFF

Approving Committee		Name
Prepared by	CS-IT	Umair Naseer
		Ammar Shahid
		Muhammad Adil Khan
Reviewed by & Endorsed by	Head of Group IT	Mohamed Sadawy
Approved by	CEO	Ayman Ahmed

## DISTRIBUTION LIST

<input checked="" type="checkbox"/> / <input type="checkbox"/>	Departments
<input checked="" type="checkbox"/>	Bukhatir Senior Management
<input checked="" type="checkbox"/>	All Employees
<input type="checkbox"/>	All Beam Creative Science School Parents and Caretakers

## CONTENTS

1.	Overview .....	4
2.	Purpose .....	4
3.	Scope .....	4
4.	Policy .....	5
4.1	General Use and Ownership.....	5
4.3	Unacceptable Use.....	6
5.	Policy Compliance .....	9
5.1	Compliance Measurement .....	9
5.2	Exceptions.....	9
6.	Related Standards, Policies and Processes: .....	10
7.	Information and Support: .....	10
8.	Appendix .....	10



<b>Name:</b> Acceptable Use	<b>Document Number:</b> BIL - IT - POL-005
<b>Department:</b> Bukhatir-IT	<b>Version Number:</b> 01
<b>Revision Date:</b> 8/March/2021	<b>Effective Date:</b> 9/March/2021

## 1. Overview

---

Group IT's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Bukhatir Group's established culture of openness, trust and integrity. Group IT is committed to protecting Bukhatir Group's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Bukhatir Group. These systems are to be used for academic / business purposes in serving the interests of the company, and of our students and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Bukhatir Group employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## 2. Purpose

---

The purpose of this policy is to outline the acceptable use of computer equipment at Bukhatir Group. These rules are in place to protect the employee and Bukhatir Group. Inappropriate use exposes Bukhatir Group to risks including virus attacks, compromise of network systems and services, and legal issues.

## 3. Scope

---

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Bukhatir Group academic work or to interact with internal networks and academic systems, whether owned or leased by Bukhatir Group, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Bukhatir Group and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Bukhatir Group policies and standards, and U.A.E laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Bukhatir Group, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Bukhatir Group.



<b>Name:</b> Acceptable Use	<b>Document Number:</b> BIL - IT - POL-005
<b>Department:</b> Bukhatir-IT	<b>Version Number:</b> 01
<b>Revision Date:</b> 8/March/2021	<b>Effective Date:</b> 9/March/2021

## 4. Policy

---

### 4.1 General Use and Ownership

4.1.1 Bukhatir Group proprietary information stored on electronic and computing devices whether owned or leased by Bukhatir Group, the employee or a third party, remains the sole property of Bukhatir Group. You must ensure through legal or technical means that proprietary information is protected in accordance with the general Data Protection Standards.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Bukhatir Group proprietary information.

4.1.3 You may access, use or share Bukhatir Group proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Bukhatir Group may monitor equipment, systems and network traffic at any time, per Group IT's Audit Policy.

4.1.6 Bukhatir Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy & other guideline

### 4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

4.2.2 System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a Bukhatir Group email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Bukhatir Group, unless posting is in the course of academic duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

### 4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Bukhatir Group authorized to engage in any activity that is illegal under local, Emirate, federal or international law while utilizing Bukhatir Group-owned resources. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

#### 4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Bukhatir Group.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Bukhatir Group or the end user does not have an active license is strictly prohibited.
3. Accessing data, server or an account for any purpose other than conducting Bukhatir Group business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).



<b>Name:</b> Acceptable Use	<b>Document Number:</b> BIL - IT - POL-005
<b>Department:</b> Bukhatir-IT	<b>Version Number:</b> 01
<b>Revision Date:</b> 8/March/2021	<b>Effective Date:</b> 9/March/2021

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Bukhatir Group computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Bukhatir Group account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Group IT is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, hotspots, or similar technology on the Bukhatir Group network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Bukhatir Group employees to parties outside Bukhatir Group.

#### 4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department. For more information please refer to email policy.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Bukhatir Group's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Bukhatir Group or connected via Bukhatir Group's network.
7. Posting the same or similar non-academic / business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
8. Condolence Email with carbon copying everyone in school is not permitted. If you want to console or condole someone please visit the him or her in person.
9. Congratulatory emails again should be only sent to the person whom you are congratulating, its neither appropriate not permitted to include other people in CC.

#### 4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Bukhatir Group's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Bukhatir Group's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Bukhatir



<b>Name:</b> Acceptable Use	<b>Document Number:</b> BIL - IT - POL-005
<b>Department:</b> Bukhatir-IT	<b>Version Number:</b> 01
<b>Revision Date:</b> 8/March/2021	<b>Effective Date:</b> 9/March/2021

Group's policy, is not detrimental to Bukhatir Group's best interests, and does not interfere with an employee's regular work duties. Blogging from Bukhatir Group's systems is also subject to monitoring.

2. Bukhatir Group's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Bukhatir Group and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Bukhatir Group's Non-Discrimination and Anti-Harassment policy.
4. Employees may also not attribute personal statements, opinions or beliefs to Bukhatir Group when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Bukhatir Group. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Bukhatir Group's trademarks, logos and any other Bukhatir Group intellectual property may also not be used in connection with any blogging activity.

## 5. Policy Compliance

---

### 5.1 Compliance Measurement

The Group IT team will verify compliance to this policy through various methods, including but not limited to, academic / business tool reports, internal and external audits, and feedback to the policy owner.

### 5.2 Exceptions

Any exception to the policy must be approved by the Group IT team in advance.



<b>Name:</b> Acceptable Use	<b>Document Number:</b> BIL - IT - POL-005
<b>Department:</b> Bukhatir-IT	<b>Version Number:</b> 01
<b>Revision Date:</b> 8/March/2021	<b>Effective Date:</b> 9/March/2021

## 6. Related Standards, Policies and Processes:

---

- Data Classification Policy
- Data Protection Policy
- Social Media Policy
- Minimum Access Policy
- Password Construction Guidelines
- Non-Discrimination and Anti-Harassment Policy.
- Email Policy

## 7. Information and Support:

---

For further information and support on this policy, contact CS-IT.

## 8. Appendix

---

Appendix No.	Form Description	Document No.