

	AL NOOR REHABILITATION & WELFARE ASSOCIATION FOR PEOPLE OF DETERMINATION  النور جمعية النور لرعاية وتأهيل أصحاب الهمم		
	POLICY		
	IT INFRASTRUCTURE		
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 1 of 17

Introduction

The Local Area Networks (LAN) systems at the Centre consisting of wired and wireless networks, are intended to provide LAN users with access to real-time information anywhere within the organization. This mobility provided by the wireless network supports productivity and service opportunities not possible with wired networks.

Purpose

The policy provides guidance to define the security controls at the Centre besides safeguarding the information technology facilities, and the Centre's network from the risk of loss or unauthorized access. This policy, through its guidelines of usage, also aims at improving the efficiency and effectiveness of job performances at the Centre.

Scope

This policy applies to the users of the IT facility of the Centre namely

- Staff
- Students
- Guests/ Visitors

Policies and Procedures

Framework of Local Area Networks

The wired network at the Centre includes firewall, Patch Panels and network switches which are connected through cables.

Prepared by: Admin & Finance Manager

Approved by: Director

			
	POLICY		
	IT INFRASTRUCTURE		
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 2 of 17

The wireless network at the Centre includes firewall, wireless controller, network switches and a number of Access points.

Firewall

A Firewall is a hardware and software device that controls access between two networks.

The intended use of firewall is to implement security features like web filtering, firewall rules, and content filtering.

The firewall shall be fixed at the Data Centre room (server room). The firewall device is configured as a Router with the internet connection from Etisalat (telecommunications service provider) being directly connected to it, giving the Centre the advantage of being able to access the full bandwidth from Etisalat.

Wireless Access Controller

A wireless LAN controller is used in combination with the Lightweight Access Point Protocol to manage light-weight access points in large quantities by the network administrator. Two Wireless Access Controllers control all access points at the Centre and work simultaneously (master-slave concept). The system implemented is such that one of the two wireless access controllers also acts as a primary controller and the other acts as a secondary controller. Should any one of the two controllers malfunction, the second one will take on the load of the malfunctioning controller

Prepared by: Admin & Finance Manager

Approved by: Director

	 AL NOOR  النور REHABILITATION & WELFARE ASSOCIATION FOR PEOPLE OF DETERMINATION جمعية النور لرعاية وتأهيل أصحاب الهمم		
	POLICY		
	IT INFRASTRUCTURE		
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 3 of 17

automatically without any downtime and therefore no hindrance to wireless connectivity.

Network Switch

Wired Lan :

The wired LAN consists of 10 network switches including 2 PoE switches which are connected to patch panels. Patch panels serve as a link between the switches and the network cables from various systems at the Centre.

The location and number of switches per location is as follows :

	Location	No. of switches
Ground Floor	Intermediate Distribution Frame IDF-1	6 (including 1 Core switch)
	Intermediate Distribution Frame IDF-2	1
First Floor	Intermediate Distribution Frame IDF-1	3

Wireless network :

Power over Ethernet(PoE) switches connect the Wireless Access Controller and the wireless Access points.

The Centre's wireless network has 6 network switches.

The location and number of the switches per location is as follows

Prepared by: Admin & Finance Manager	Approved by: Director
--------------------------------------	-----------------------

			
POLICY			
IT INFRASTRUCTURE			
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 4 of 17

Location		No. of switches	Switch Code
Ground Floor	Intermediate Distribution Frame IDF-1	1 -2 "Core Switch"	GF IDF-1 SW1 GF IDF-1 SW2
	Intermediate Distribution Frame IDF-2	2	GF IDF-2 SW-1 GF IDF-2 SW-2
First Floor	Intermediate Distribution Frame IDF-1	2	FF IDF SW1 FF IDF SW2

By default, new access controller is licensed to connect 500 access points. An additional 150 licenses (lifetime licenses – need no renewals) imported to the access to controllers enable the connection of all access points to the 2 controllers.

Wireless Access Points

The Wireless Network consists of a total of 103 Access Points positioned at various locations at the Centre - 46 Access Points on the Ground floor and 47 on the First Floor. 10 access points positioned in parking and other outside area.

S/No	ACCESS POINT	IDF No.
1	GF AP- G20	GF IDF1
2	GF AP- G01	GF IDF1
3	GF AP- G03	GF IDF1
4	GF AP- G04	GF IDF1
5	GF AP- G05	GF IDF1
6	GF AP- G06	GF IDF1

Prepared by: Admin & Finance Manager	Approved by: Director
--------------------------------------	-----------------------

POLICY

IT INFRASTRUCTURE

Document No. POL/IT/13

Rev:04

Date Of Issue: 24 November 2025

Page 5 of 17

7	GF AP- G07	GF IDF1
8	GF AP- G09	GF IDF1
9	GF AP-G10	GF IDF1
10	GF AP- G11	GF IDF1
11	GF AP- G12	GF IDF1
12	GF AP- G17	GF IDF1
13	GF AP- G20	GF IDF1
14	GF AP- G22	GF IDF1
15	GF AP- G24	GF IDF1
16	GF AP- G18	GF IDF1
17	GF AP- G19	GF IDF1
18	GF AP- G21	GF IDF1
19	GF AP-G02	GF IDF1
20	GF AP- G13	GF IDF1
21	GF AP- G16	GF IDF1
22	GF - AP 95	GF IDF1
23	GF AP- 93	GF IDF1
24	GF AP 94	GF IDF1
25	GF AP 91	GF IDF1
26	GF AP 103	GF IDF1
27	GF AP 97	GF IDF1
28	GF AP 104	GF IDF1
29	GF AP-98	GF IDF1
30	GF AP 96	GF IDF1
31	FF AP-F35	GF IDF2
32	FF AP- F49	GF IDF2
33	FF AP- F34	GF IDF2
34	FF AP- F64	GF IDF2
35	GF AP- G30	GF IDF2
36	GF AP- G29	GF IDF2
37	GF AP-G44	GF IDF2
38	GF AP- G43	GF IDF2
39	GF AP- G40	GF IDF2

Prepared by: Admin & Finance Manager

Approved by: Director

POLICY

IT INFRASTRUCTURE

Document No. POL/IT/13

Rev:04

Date Of Issue: 24 November 2025

Page 6 of 17

40	GF AP- G30	GF IDF2
41	FF AP- F36	GF IDF2
42	GF AP- G25	GF IDF2
43	GF AP- G26	GF IDF2
44	BF AP- G28	GF IDF2
45	GF AP- G33	GF IDF2
46	GF AP- G34	GF IDF2
47	GF AP-G35	GF IDF2
48	GF AP- G37	GF IDF2
49	GF AP- G40	GF IDF2
50	GF AP- G41	GF IDF2
51	GF AP- G32	GF IDF2
52	FF AP- F31	GF IDF2
53	FF AP- F44	GF IDF2
54	FF AP- F39	GF IDF2
55	FF AP- F40	GF IDF2
56	FF AP- F42	GF IDF2
57	FF AP- F43	GF IDF2
58	FF AP- F32	GF IDF2
59	FF AP-F30	GF IDF2
60	FF AP-F29	GF IDF2
61	FF AP-F33	GF IDF2
62	GF AP-G31	GF IDF2
63	GF AP-G27	GF IDF2
64	GF AP-GF40	GF IDF2
65	OD AP 99	GF IDF2
66	OD AP100	GF IDF2
67	OD AP101	GF IDF2
68	OD AP102	GF IDF2
69	FF AP-F02	FF IDF1
70	FF AP-F62	FF IDF1
71	FF AP-F59	FF IDF1
72	FF AP-F01	FF IDF1

Prepared by: Admin & Finance Manager

Approved by: Director

POLICY

IT INFRASTRUCTURE

Document No. POL/IT/13

Rev:04

Date Of Issue: 24 November 2025

Page 7 of 17

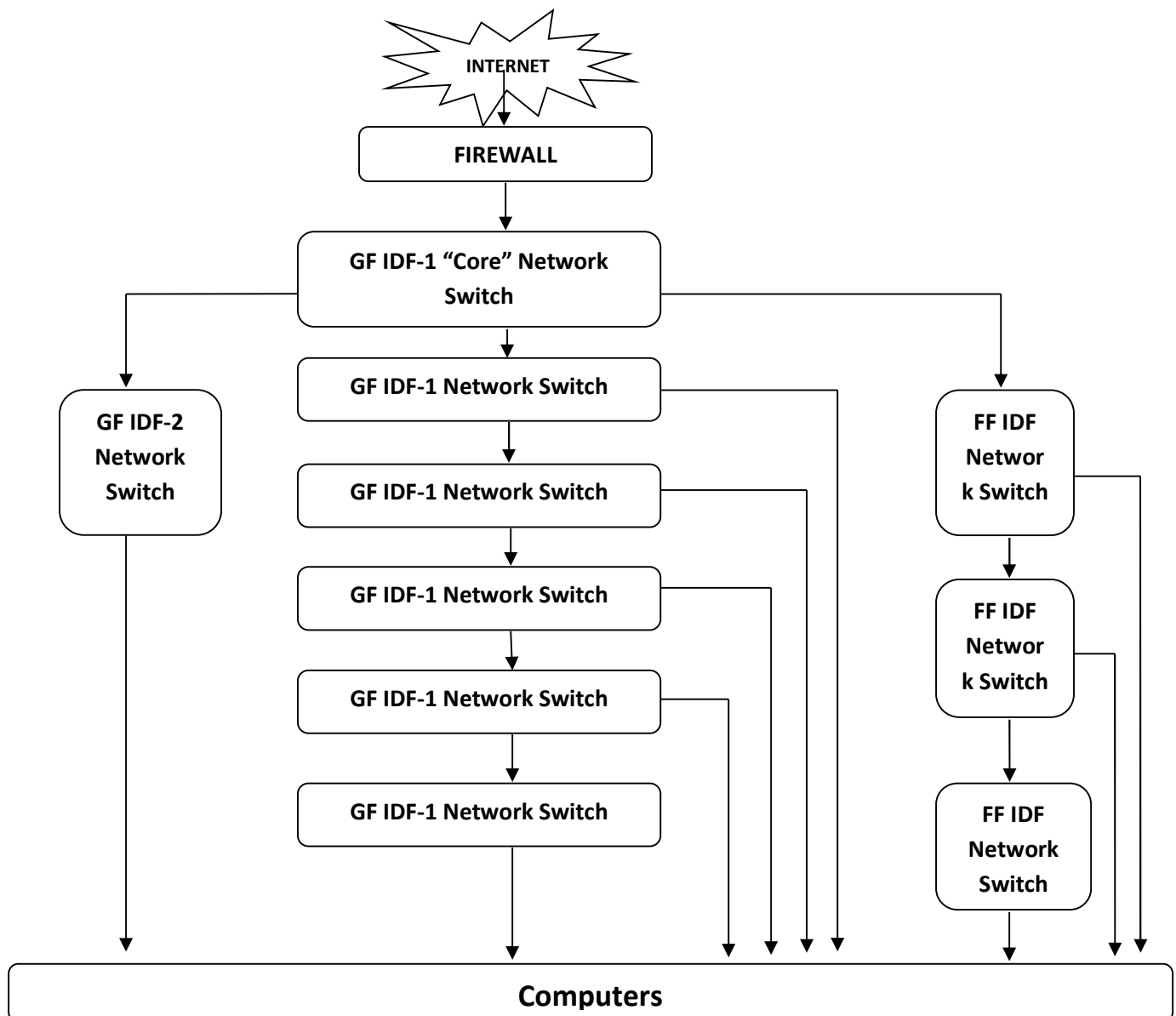
73	FF AP-F24	FF IDF1
74	GF AP-G27	FF IDF1
75	FF AP-F52	FF IDF1
76	FF AP-F07	FF IDF1
77	FF AP-F37	FF IDF1
78	FF AP-FF51	FF IDF1
79	FF AP-F10	FF IDF1
80	FF AP-F11	FF IDF1
81	FF AP-F12	FF IDF1
82	FF AP-F13	FF IDF1
83	FF AP-F14	FF IDF1
84	FF AP-F15	FF IDF1
85	FF AP-F16	FF IDF1
86	FF AP-F17	FF IDF1
87	FF AP-F18	FF IDF1
88	FF AP-F19	FF IDF1
89	FF AP-F20	FF IDF1
90	FF AP-F21	FF IDF1
91	FF AP-F22	FF IDF1
92	FF AP-F23	FF IDF1
93	FF AP-F25	FF IDF1
94	FF AP-F26	FF IDF1
95	FF AP-F27	FF IDF1
96	FF AP-F28	FF IDF1
97	FF AP-F09	FF IDF1
98	FF AP-F04	FF IDF1
99	FF AP-F06	FF IDF1
100	FF AP-F05	FF IDF1
101	FF AP-F08	FF IDF1
102	FF AP-F03	FF IDF1
103	FF AP-F47	FF IDF1

Prepared by: Admin & Finance Manager

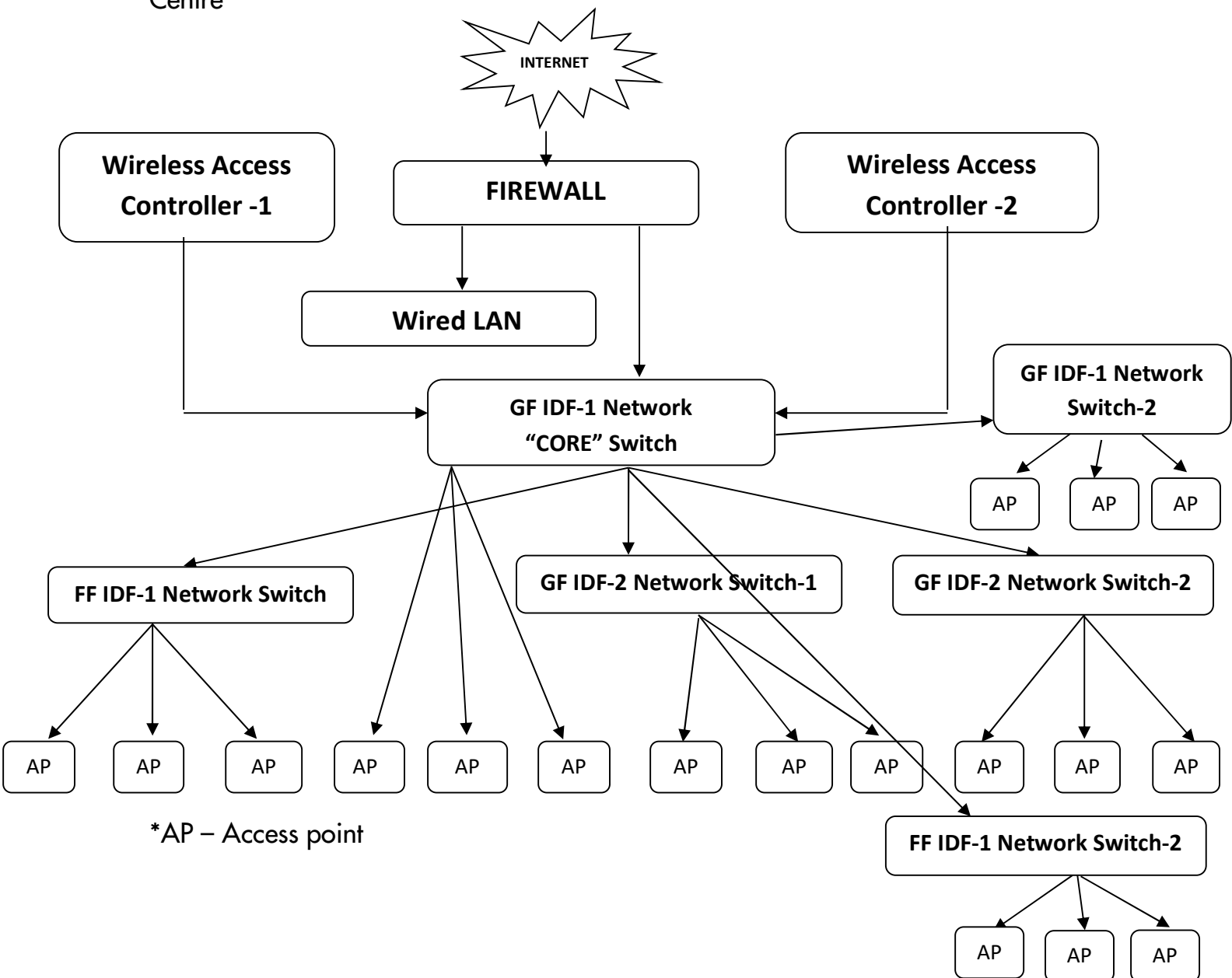
Approved by: Director

Local Area Network Infrastructure

The diagram below shows the wired network infrastructure implemented at the Centre



The diagram below shows the wireless network infrastructure implemented at the Centre



Prepared by: Admin & Finance Manager

Approved by: Director

			
	POLICY		
	IT INFRASTRUCTURE		
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 10 of 17

Network Security Policy

The below policy outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of network security environment

Wired System

Access of the Centre's systems (laptops and desktops) to the Wired Network shall be under the control of the IT executive who shall also be the IT Administrator at the Centre. The IT Administrator shall authorize the connection of such devices to the Al Noor domain.

Wireless System

Access to the Wireless Network shall be under the control of the IT executive who shall also be the IT Administrator at the Centre.

Service Set Identifiers (SSIDs)

Three categories (SSIDs) shall be made available on the Centre's Wireless Network namely

- Al-Noor-Student
- Al-Noor-Staff
- Al-Noor-Guest

Prepared by: Admin & Finance Manager	Approved by: Director
--------------------------------------	-----------------------

			
POLICY			
IT INFRASTRUCTURE			
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 11 of 17

1. Al-Noor-Staff

All the Centre's laptops, by default, shall connect automatically to the Centre's wireless network

Access to Wi-Fi may be made available on personal devices such as laptops, mobiles and other handheld devices of staff in the following categories only

- Director
- Program Leaders
- HODs
- Assistant HODs
- SCR department
- Admin & Finance department
- Special Educators and Therapist

The IT executive shall seek the approval of Admin manager prior to providing access to staff personal devices and maintain a record of staff personal devices connected to the wireless network.

2. Al-Noor-Guest Guests/visitors may be enabled to access the Centre's wireless through a password

PASSWORDS

All the SSIDs shall be encrypted and must meet complexity requirements as follows

- minimum 6 characters
- At least one uppercase letter or lower case letter needed
- At least one special characters or special symbols

Prepared by: Admin & Finance Manager	Approved by: Director
--------------------------------------	-----------------------

			
	POLICY IT INFRASTRUCTURE		
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 12 of 17

Staff and Students password shall be changed every 12 months preferably during the months of December/January.

Guest password shall be changed every month

The IT executive shall be the custodian of all passwords at the Centre. A copy of all passwords shall be made available to the admin manager. Any revisions to passwords shall be notified to the admin manager, prior to the change and a revised list of passwords be provided immediately.

SSID Passwords may not be conveyed to any member of staff, students or guests without the approval of the Admin Manager.

USER LOGIN:

Staff shall be provided with user IDs in order to connect to the Al Noor network. Passwords to staff accounts should not be known by anyone but the staff member. If a password is lost or forgotten, system administrators shall assist in securing a new password. Such user login passwords shall be changed annually.

CATEGORIES BLOCKED BY FIREWALL

Accessibility to the following categories of internet sites shall be blocked by Firewall:-

- Criminal Potential
 1. Hacking
 2. Criminal Skills
 3. Malicious
 4. Violence

Prepared by: Admin & Finance Manager	Approved by: Director
--------------------------------------	-----------------------

			
POLICY			
IT INFRASTRUCTURE			
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 13 of 17

5. Plagiarism
 6. Remote access
- Sexuality (All porn related sites)
 - Torrent Applications

Further internet accessibility controls shall be implemented using Trend Micro software firewall which shall restricted access to internet sites as mentioned below

<u>Category</u>	<u>Restricted</u>	<u>Allowed</u>
Adult	Adult/Mature Content	none
	Pornography	
	Sex Education	
	Intimate Apparel/Swimsuit	
	Nudity	
	Alcohol	
	Illegal	
	Tasteless	
	Gambling	
	Violence/Racism	
	Abortion	
	Weapons	
	Illegal drugs	
Business	Brokerages\Trading	Business\Economy
	Shopping	Financial Services
	Auction	Job Search\Careers
	Real Estate	
Communication and Search	Internet Telephony	Search Engines\Portals
	Blogs\Web Communication	Email
	Social Networking	News Group

Prepared by: Admin & Finance Manager

Approved by: Director

 AL NOOR REHABILITATION & WELFARE ASSOCIATION FOR PEOPLE OF DETERMINATION  النور جمعية النور لرعاية وتأهيل أصحاب الهمم			
POLICY			
IT INFRASTRUCTURE			
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 14 of 17

	Chat\Instant Messaging	Web Hosting
		Internet Infrastructure
General	Military	News\Media
	Politics	Translators\Cached Pages
	Health	Reference
	Computers\Internet	Education
	Vehicles	Government\Legal
	Unrated	
Internet Security	Proxy Avoidance	none
	Malicious Software	
	Spyware	
	Spam	
	Adware	
	Malware	
	Disease Vector	
	Cookies	
	Dialers	
	Hacking	
	Joke Program	
	Password Cracking	
	Remote Access Program	
	Web Advertisement	
Lifestyle	Recreation/Hobbies	Games
	Arts	Journals
	Entertainment	Restaurants\Food
	Cult\Occult	For Kids
	Cultural Institutions	
	Activist Groups	
	Personals\Dating	
	Religion	
	Personal Sites	

Prepared by: Admin & Finance Manager	Approved by: Director
--------------------------------------	-----------------------

AL NOOR REHABILITATION & WELFARE ASSOCIATION FOR PEOPLE OF DETERMINATION  الـنـور جمعية النور لرعاية وتأهيل أصحاب الهمم			
POLICY			
IT INFRASTRUCTURE			
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 15 of 17

	Social Lifestyle	
	Gay/Lesbian	
	Gun clubs\Hunting	
	Travel	
	Humor	
Network Bandwidth	Internet Radio and TV	Photo Searches
	Personal Network Storages	
	Peer to Peer	
	Streaming Media/MP3	
	Ringtones/Mobile Phone Downloads	
	Software Downloads	
	Pay to Surf	

The above restricted access shall be provided to all users.
Full access or access to social networking sites and media streaming may be provided to specific staff on the basis of job requirements and upon the written approval of the Director only.

Prepared by: Admin & Finance Manager	Approved by: Director
--------------------------------------	-----------------------

			
POLICY			
IT INFRASTRUCTURE			
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 16 of 17

Appendix – Amendment History & Authorisation

Revision No	Description of Change	Issue Date	Authorised By
00	First Issue	01 Sept 2014	Director
01	New Al Noor logo	01 Feb 2016	Director
02	Replace the Centre's logo in all QMS documents and revision of document codes	12 Aug 2020	Director
03	Change 1. Change in Department name & designation 2. Centre's wireless network from 4 to 6 network Switches 3. By default, new access controller is licensed to connect 500 access points. An additional 150 licenses (lifetime licenses – need no renewals) imported to the access to controllers enable the connection of all access points to the 2 controllers. 4. Added new Access point list	27 November 2024	Director
04	Deletion of the below content from the POLICY - IT INFRASTRUCTURE Document No. POL/IT/13 Al-Noor-Student Requests for connection of devices to the wireless network for student usage shall be approved by the HOD/Assistant HOD of the IT- teaching department using the prescribed format and be forwarded to the IT executive. Students' Personal devices may also be connected to wireless system. All student devices (personal and/or Al Noor's) shall be registered before providing access to the wireless network. The IT executive shall maintain a register of student devices that are connected to the network and shall include the following details : - Date of registration	24 November 2025	Director

Prepared by: Admin & Finance Manager

Approved by: Director

 AL NOOR REHABILITATION & WELFARE ASSOCIATION FOR PEOPLE OF DETERMINATION  النور جمعية النور لرعاية وتأهيل أصحاب الهمم			
POLICY			
IT INFRASTRUCTURE			
Document No. POL/IT/13	Rev:04	Date Of Issue: 24 November 2025	Page 17 of 17

	- Device belongs (whether personal or Al Noor's) - Details of the device (brand, type and asset code of belonging to Al Noor) - Approved by (name and designation of the approving authority) Once registered, such devices may be connected to the wireless network automatically. Record of Centre's and students' devices which are connected to the wireless network shall be also maintained by the IT (teaching) department. Reason for change: As the Centre aligns its tech services with the UAE leadership's mandate and embraces AI in a major way, it has been encouraging parents to procure personal digital devices for students for purposes of communication, learning, IEP implementation etc.. BYOD has been recommended for several students as it enables customization and personalization of settings and features while also working on operational competency skills, online safety skills, etc. It will become logistically intense and unmanageable to register each student device before providing access to the Centre's wireless network. Hence it is deemed impractical to have a stipulation in the policy that cannot be implemented.		
--	---	--	--

Prepared by: Admin & Finance Manager	Approved by: Director
--------------------------------------	-----------------------