

			
	POLICY		
	REMOTE ACCESS TO AL NOOR NETWORK		
Document No. POL/IT/40	Rev:03	Date Of Issue: 01 October 2026	Page 1 of 3

Introduction

Remote Access is the ability to get access to a network from a remote distance. This allows an employee to work offsite such as from home or in other locations while still having access to his/her network.

Purpose

This policy is designed to provide access to the organization's files stored on the network.

Scope

This policy applies to all staff of the Centre. This policy also covers all technical implementations of remote access used to connect to the Centre's network

Policy

Remote Access is mainly Application based access

- **Application Based Access**
Application based access provides access to e-Response Recording Logs(eRRLs) shared files through the installation of a Hardware Firewall (Fortinet 100F) at the Centre. DynamicDNS service is configured with this firewall to access the network through a VPN application (FortiClient) installed on the user's laptop.

Rights:

All Program Leaders and HODs shall have emote access to emails and eRRLs

Remote access shall be limited to eRRLs through the application for all teachers and therapists. Further permission may be granted at the Management discretion

Installation of the application shall be done by the IT Administrator. The application may be installed on personal laptops of staff subject to approval from the respective HODs and Coordinators only. The IT executive shall maintain a register of such personal laptops and

			
	POLICY		
	REMOTE ACCESS TO AL NOOR NETWORK		
Document No. POL/IT/40	Rev:03	Date Of Issue: 01 October 2026	Page 2 of 3

provide individual usernames and passwords. Access to the application on a personal laptop shall be through the individual log in(username) which shall be deleted should the staff member resign.

Application log-in for staff using the Centre's laptops shall be through a username and password provided by IT department.

PROCEDURE

ACCESS TO eRRLs

- Application based :

Open the FortiClient application on the desktop and connect with the given username and password

User name: xxxx

Password: xxxxx

When connected, users can use the eRRL shortcut icon created on their desktop. It is recommended that users disconnect the application when done.

			
POLICY			
REMOTE ACCESS TO AL NOOR NETWORK			
Document No. POL/IT/40	Rev:03	Date Of Issue: 01 October 2026	Page 3 of 3

Appendix – Amendment History & Authorisation

Revision No	Description of Change	Issue Date	Authorised By
00	First Issue	30 Jan 2017	Director
01	Replace the Centre's logo in all QMS documents and revision of document codes	12 Aug 2020	Director
02	Change 1. Web based Access allowed for use by Program Leaders & HOD 2. Fortinet from 100D to 100F 3. From OWA to Microsoft Office 365:Login	27 November 2024	Director
03	Web based access was used to reach Al Noor email on the on-premise server. Email is now on Microsoft 365, so this access is no longer used, and all remote email references have been removed. Summary of changes: 1. Purpose: "and/or emails" removed; the policy now covers access to files stored on the network only. 2. Policy – categories: "two categories: Web based and Application based access" changed to "mainly Application based access". 3. Policy – Web based Access to Emails: section removed. 4. Policy – Application Based Access: "emails and" removed (eRRRLs only); "DynDNS" changed to "DynamicDNS". 5. Policy – Rights: "Coordinators" changed to "Program Leaders"; "therapists and therapist" to "teachers and therapists"; Centre laptop log-in changed from "a common username" to "a username and password provided by IT department". 6. Procedure: Section 1 "Access to Emails" (web portal and application based) removed; "Access to eRRRLs" is now the only procedure.	01 October 2026	Director