OFFLINE RESILIENCE GUIDE // UK EDITION

Build a Small Offline Information Server

Use an old laptop, Raspberry Pi or mini PC to serve household documents and reference pages over your own local network — without exposing it to the public internet.

OFFLINE REFERENCE | UPDATED 30 SEP 2026 | UK FOCUS

> PDF edition generated 13 October 2026 from the GPN website release v12.21.16. The individual guide editorial review dates appear below. This is a saved reference, not a live safety warning or a fresh independent source verification. When online, check current official advice.

LAYER 1 // ACT

FIELD CARD

Immediate actions first. Then read the conditions and limits below.

FIRST ACTIONS

- Start with a folder of static HTML/PDF/text files; complexity is optional.
- Give the server a predictable local address, preferably using a DHCP reservation on the router.
- Serve only to the LAN unless you deliberately know how to secure an internet-facing service.
- Keep a second offline copy of irreplaceable documents; the server is an access point, not the only backup.

DO NOT

- Do not port-forward the server to the public internet by default.
- Do not store a household medical dossier, passwords or other highly sensitive personal data on a broadly shared server.
- Do not rely on one SD card or one computer as the sole copy of important information.

IF THIS HAPPENS

- If the internet is down but the router is powered, browse directly to the server’s local IP address.
- If the router is unavailable, a technically confident user can build a standalone access point, but test that configuration in advance rather than improvising during an incident.

WHAT YOU NEED

- Low-power computer
- Storage with a backup copy
- Local router/switch or tested standalone network
- Simple web server or file share
- Printed local address/instructions

> **BOUNDARY**
> This is a practical reference aid. Current official instructions, emergency services, competent professionals and product documentation take priority where they conflict.

The simplest useful version

The smallest useful “server” is just a low-power computer that stores files and presents them to other devices on the LAN. Static HTML is ideal because it needs almost no processing and remains readable in any browser. You can also keep PDFs, text manuals, exported contacts, offline maps and a community bulletin page.

Choose boring hardware

An old laptop has a screen, keyboard and built-in battery, which can make it unusually resilient. A Raspberry Pi is compact and efficient. A mini PC offers more storage and performance. The best choice is the machine you already understand, can power safely and can repair or replace. Avoid creating a specialist appliance that nobody else in the household knows how to use.

Serve a static folder

On Raspberry Pi OS, the official documentation describes installing Apache to serve local webpages. Other simple choices exist on Windows, macOS and Linux. The principle is the same: put static files in a web root, start the service, and browse to the machine’s local IP address from another device. Keep the stack minimal; a household reference library does not need a database.

Make the address predictable

Use the router’s DHCP reservation feature so the server normally receives the same local address. Give it a clear hostname if your network resolves local names, but also print the numeric address because local name resolution can fail. Put the address on the server case or a paper household plan.

What to host

Useful content includes a GPN static/offline copy, appliance and equipment manuals, scanned emergency plans, non-sensitive contact sheets, local council and utility phone numbers, public first-aid references, offline maps, a simple bulletin page and files that neighbours or household

members may need. Keep personal identifiers and sensitive medical details off a shared server unless access control and the need are properly considered.

Security boundary

A service reachable only from your trusted LAN has a smaller exposure than a public internet service, but it still needs updates, strong accounts and sensible permissions. Raspberry Pi’s operational-security guidance recommends current software and firewall controls. Disable services you do not need. Do not enable router port forwarding or UPnP exposure for convenience.

Backups and checksums

The server should not be the archive of last resort. Keep a second copy on a removable drive stored separately, and optionally a third copy on another device. A checksum such as SHA-256 can help confirm that a large archive has not silently changed; store the checksum list alongside the backup. A checksum proves file consistency, not trustworthiness or freshness.

Test the failure mode

Disconnect the internet/WAN while leaving the LAN powered. From a phone or laptop, open the local server, download a document and follow a local link. Then reboot the server and confirm the service starts automatically. If those steps do not work during a calm test, they are unlikely to improve during an outage.

Verify / learn

These references are resolved from GPN’s central source registry so authority, coverage and source changes can be managed in one place. If a current official source conflicts with this guide, follow the current official source.

> **TECHNICAL / REFERENCE SOURCE**
> **Raspberry Pi remote-access and web-server documentation**
> Example project documentation. Secure configuration and software maintenance remain the operator’s responsibility.
> https://www.raspberrypi.com/documentation/computers/remote-access.html

> **TECHNICAL / REFERENCE SOURCE**
> **Raspberry Pi operational security**
> Applies to Raspberry Pi systems; equivalent controls vary on other platforms.
> https://www.raspberrypi.com/documentation/security/operational-security.html

> **TECHNICAL / REFERENCE SOURCE**
> **Raspberry Pi networking documentation**
> Device/project documentation; router interfaces and other operating systems differ.
> https://www.raspberrypi.com/documentation/computers/configuration.html

Editorial review date: 30 September 2026. Next scheduled review: 28 January 2027.

INFORMATION CHECK✓ CURRENT REVIEW

REVIEWED	NEXT REVIEW DUE	REGISTERED REFERENCES
30 Sep 2026	28 Jan 2027	3 sources

Source availability is not hazard status. Offline reference material must never be interpreted as a live all-clear.

GET PREPPED NOW // ORIGINAL GUIDE

Source page: https://getpreppednow.co.uk/guides/offline-information-server.html
Editorial update: 30 September 2026 · © 2026 Get Prepped Now
Personal household printing and offline saving are permitted. Keep this attribution and the guide's source/review information with the copy. Copyright & permitted use