

Overview of Visitor WiFi Service

The Challenge

Providing WiFi to transient visitors is a significant challenge faced by many HEAnet client sites. Amongst the concerns that arise are:

1) Reputational damage

A local AUP may be inadequate when trying to moderate behaviour of visitors who have no formal relationship with your organisation. Any malicious online activity by visiting users of your local WiFi will be traced back in the first instance to an IP address in your range.

Should a serious incident occur, legal and/or media attention may reference the organisation responsible for that IP address, generating adverse publicity for your institution even where you are not found legally responsible for the malicious activity.

2) End-user support

Transient visitors, many of whom may have no technical knowledge, have the potential to consume significant helpdesk support resources when registering with the service, configuring their mobile devices, troubleshooting issues, etc. Providing support outside of normal business hours is a particular challenge.

Providing a good quality user experience instils users with a positive view of the institution and is also a valuable way of engaging with visitors e.g. providing course information for potential future students.

3) Accountability

In order that users of the visitor WiFi can be held accountable for their online actions, you need to be able to uniquely identify them. This requires that you record identifying details for each visitor, and be able to trace activity back to each one.

Any system to support these requirements incurs a management overhead and also imposes the burden of legal obligations around data protection and data retention.

4) Legal protection

HEAnet and its clients provide network connectivity exclusively for the Irish research and academic community. As the general public may be amongst the users of a visitor WiFi service, the service architecture must ensure that relevant obligations on a private and publicly funded network continue to be met.

The Solution

A visitor WiFi service managed by a third-party provider addresses all of these concerns.

The visitor WiFi service piggybacks on your existing WiFi equipment. All traffic to/from visitors is transported to the third-party provider within an encrypted tunnel across the HEAnet backbone. The third party provider becomes the WiFi service provider, taking on all of the responsibilities that this implies (registering and authenticating users of the service, providing IP addresses to visitor devices, routing traffic onwards, end-user support, etc.).

HEAnet have established a non-exclusive agreement with a third-party provider to offer a brokered service based on this model. Please contact us for further details at noc@heanet.ie.