



Response Date: 11/06/2025

2025/419 - Contracts

In response to your recent request for information regarding;

- 1. Please state how many contracts the department has signed with Pen-Link Technologies UK Ltd or its parent company Cobwebs Technologies Ltd. Please also search for "Cobwebs Technologies UK Ltd" as this is the former name of Pen-Link Technologies UK Ltd.**

For each contract please state its

- a. name**
- a. award date**
- a. start date**
- a. end date**
- a. financial value**

For each contract, please also state what services are/were provided under the contract.

For each contract, please also state whether you have, or had, access to the product 'Webloc' under the contract.

For each contract, please state how it was awarded (e.g. through competitive tender, direct award, called off a framework agreement).

Any disclosure under FOI is a release to the public at large. Under the Act, we cannot, and do not request the motives of any application for information. We have no doubt that the vast majority of requests made under the Act are legitimate and the applicants do not have any ulterior motives. Whilst not questioning the motives behind this specific request, confirming or denying that information is held regarding business with PENLINK, or any other likeminded third-party provider, would cause operational harm and affect our ability to fulfil our core function of law enforcement in the future. Confirming or denying whether or not information is held would enable individuals and organisations that are intent on causing disruption to identify strengths and weaknesses at force level, and more so nationally, which could be exploited causing harm to members of the public. This would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public.

The threat from terrorism cannot be ignored. It is generally recognised that the international security landscape is increasingly complex and unpredictable. Since 2006, the UK Government has published the threat level based upon current intelligence, and that threat is currently judged as "[SUBSTANTIAL](#)", meaning that an attack on the UK is likely. It is well established that police forces use tactics and technology to gain intelligence in order to counteract criminal behaviour, and it has

Pencadlys yr Heddlu,
Glan-y-Don, Bae Colwyn LL29 8AW
www.heddlugogleddcymru.police.uk

Police Headquarters,
Glan-y-Don, Colwyn Bay LL29 8AW
www.northwales.police.uk

been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means.

Confirming or denying whether any information is held about a contract with PENLINK and the services used would limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling offenders to take steps to counter them. It may also suggest the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing potential vulnerabilities.

This detrimental effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on disrupting policing functions throughout the UK will be able to 'map' where the use of specific businesses, their products or certain tactics may or may not be deployed. This can be useful information to those committing (or those intent on committing or planning) crime.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement.

Public Interest Test

Factors favouring Confirming or Denying for Section 24 - The information, if held, only relates to national security and confirming or denying whether it is held would not actually harm it. The public are entitled to know what public funds are spent on and what measures are in place. By confirming or denying if business is conducted with PENLINK, or any other likeminded third-party provider, would lead to a better informed public.

Factors against Confirming or Denying for Section 24 - By confirming or denying whether any information is held would render policing and security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.

Factors favouring Neither Confirming or Denying for Section 31 - Confirming or denying whether business is conducted with PENLINK, or any other likeminded third-party provider, would provide an insight into the Police Service. This would enable the public to have a better understanding of the effectiveness of the police and about how the police gather intelligence. It would greatly assist in the quality and accuracy of public debate, which could otherwise be steeped in rumour and speculation. Where public funds are being spent, there is a public interest in accountability and justifying the use of public money.

Factors against Confirming or Denying for Section 31 - Confirming or denying that any information is held regarding business with PENLINK, or any other likeminded third-party provider, would have the effect of compromising law enforcement tactics. It has been recorded that FOIA releases are monitored by criminals and terrorists and so to confirm or deny information is held concerning intelligence gathering would lead to law enforcement being undermined. The Police Service is reliant upon all manner of techniques during operations and the public release of any modus operandi employed, if held, would prejudice the ability of the Police Service to perform the functions it exists to provide.

By confirming or denying that a business interest exists would hinder the prevention or detection of crime. The Police Service would not wish to reveal what tactics may or may not have been used to gain intelligence as this would clearly undermine the law enforcement and investigative process. This would impact on police resources and more crime and terrorist incidents would be committed, placing individuals at risk. It can be argued that there are significant risks associated with providing information, if held, in relation to any aspect of investigations or of any nation's security arrangements so confirming or denying that information is held, may reveal the relative vulnerability of what we may be trying to protect.

Decision

The security of the country is of paramount importance and North Wales Police will not divulge whether any information is or is not held regarding business with any company, if to do so would place the safety of an individual at risk, undermine National Security or compromise law enforcement.

Whilst there is a public interest in the transparency of policing operations and providing assurance that North Wales Police is appropriately and effectively engaging with the threat posed by various groups or individuals, there is a very strong public interest in safeguarding the integrity of police investigations and all areas of operations carried out by police forces throughout the UK.

As much as there is public interest in knowing that policing activity is appropriate and balanced this will only be overridden in exceptional circumstances. The use of technology can be a sensitive issue that would reveal police tactics and therefore it is our opinion that for these issues the balancing test for confirming or denying whether any information is held regarding the police, PENLINK, or any other likeminded third-party provider, is not made out.

However, this should not be taken as necessarily indicating that any information that would meet your request exists or does not exist.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 08/04/2025