Privacy Notice

Name of Process: Cisco Umbrella Web Filter
Description of Process: Cloud-based web filtering solution which operates at the Domain Name System (DNS) layer. The web filter is configured with a policy which prevents access to certain categories of website, as well as preventing the downloading of content from sites which are known to be dangerous.

Data Controller	Edinburgh Napier University
Purposes for collection/processing	Information about your web browsing activity is collected and stored for a limited period of time so that it can be investigated by authorised individuals should there be a need to do so, for example during the course of investigating an information security incident or suspected breach of University policies. Further information can be found in the [Monitoring and Logging Policy](#). Aggregated browsing data is also used in the production of reports for Information Services staff and University senior managers. These reports typically show the most frequently used web applications, the most popular categories of websites visited, etc.
Legal basis	Art 6(1)(f), legitimate interests, is the main basis for processing as it is in the legitimate interests of the Controller to protect its information systems from misuse. By ensuring that all web activity can be traced to an identifiable individual, any claims of misuse or inappropriate behaviour can be investigated. Art 6(1)(c), compliance with a legal obligation, is also used as the basis for processing, since the Controller may be subject to requests for data from authorities for which there is a legal requirement to provide any available information.
Whose information is being collected	Students, staff, third-party contractors, visitors and anyone else who engages in web browsing activity on the University's wired and wireless networks.
What type/classes/fields of information are collected	• Your username • Your IP address
Who is the information being collected from	The information is being collected from you, through your use of computing devices

	connected to the University's wired and wireless networks.
Who is personal data shared with externally	Cisco Systems, Inc. Amazon.com, Inc.
How long is the information kept for	DNS query data, HTTP traffic and summarised log data is deleted no later than 2 years after initial collection. Active Directory, configuration and tracking data is not deleted unless requested.
Will the data be used for any automated decision making	Your information may be used to send you an automated notification in the event that the service detected and blocked risky or dangerous web browsing activity associated with you.
Is information transferred to a third country? Outside the EEA and not included in the adequate countries list.	Normally the data centre in which the traffic is routed will be the closest physical location to the individual initiating the DNS query, however it can be routed to any data centre facility used by Cisco Umbrella. Additionally, certain information is processed for the purposes of Cisco global threat intelligence research, such processing is conducted in the United States only.

You can access all the University's privacy notices using the following link:
https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/statement.aspx
You have a number of rights available to you with regards to what personal data of yours is held by the University and how it is processed – to find out more about your rights, how to make a request and who to contact if you have any further queries about Data Protection please see the information online using the following URL:
https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/default.aspx