eduroam(UK) Policy

Document MF-POL-003

Issue 5, June 2018

Management Summary

Jisc aims to foster collaboration between organisations whether publicly or privately funded that provide, support or collaborate in the delivery of education and research, and other public-sector organisations delivering public services, by facilitating roaming network access for members of such organisations. Provision of the federated eduroam service (the Service) is a major component in the fulfilment of this aim and is facilitated and governed in the UK by Jisc as eduroam(UK).

This Policy outlines the requirements placed upon all UK participants in eduroam, including individuals who use the service and the organisations providing the various service elements, i.e. the organisations issuing credentials (Home organisations), organisations providing network services (Visited organisations) and the operators of eduroam(UK), to ensure that each of these can be relied upon to play their part in ensuring the Service works effectively and securely. This is essential if the mutual trust required for the Service to function is to be maintained. **All users and providers of the Service are required to comply with this Policy. In cases of persistent breach of this Policy eduroam(UK) reserves the right to the bar organisations and individuals from the Service.** In addition**,** participating organisations must ensure that their computing regulations provide for individuals who breach this Policy to be subject to an appropriate disciplinary process *irrespective of their location at the time of the breach.*

The technical sanctions available to the organisations providing each service element are described below; these sanctions provide the ability to impose technical controls for the protection of the other parties and the Service against those who represent an immediate threat.

Introduction and Rationale

The primary function of eduroam is to enable individuals, whether at the home institution or when visiting another campus, to obtain access to the Internet (which in most cases will be via the Janet network) through the use of the same authentication mechanism and credentials regardless of location and without any administrative effort at the visited site. Such sharing of network services with seamless connectivity is to the mutual benefit of all participating organisations throughout the whole education and research community.

Participation in eduroam is entirely voluntary so the benefits to organisations must outweigh any difficulties that might result from providing the Service. The continuing success of the initiative and further expansion and widening of availability of the Service therefore depends on co-operation and responsible behaviour from all participants with the aims being the avoidance of disruption and overburdening of organisations and the prompt and effective resolution of any problems, particularly for participants offering a Visited service. The eduroam service is predicated on mutual trust between participating organisations; connection of roaming users to network services by Visited service members is undertaken on trust that the Home organisation faithfully authenticates the identity of the user and maintains sufficient logs to enable compliance with AUP and Security policies.

This eduroam(UK) Policy has been designed to meet the need for a policy which addresses these concerns and which must be accepted by all parties.

In addition to the above, visiting users should appreciate that their network access is a privilege, not a right, and must make best endeavours to abide by all policies that both Home and Visited organisations apply. It should be noted that each organisation has its own individual Acceptable Use Policy for its network to accommodate local technical or organisational concerns, and this may well result in different rules applying to the guest service provided by different organisations. Therefore visitors should read and accept the policies for each organisation whose eduroam services they use, wherever this is possible and the service-providing organisation can be identified, either before or early in their use of its network. (Visited organisations are required to make their local policies easily accessible, for example via their eduroam service information web page or their network access notices). In any case this eduroam(UK) Policy requires that visitors immediately cease any activity that they are informed breaches local policy.

The Policy

Users

- Are accountable to the organisations that issue them with their credentials (and to the law) for all use of such credentials and any activities undertaken with the authority of those credentials. In particular, users must not allow their own credentials, or network access authenticated by them, to be used by others. If the user believes that their credentials may have been compromised the user concerned must immediately report this to their home organisation;
- Must abide by restrictions applied by the home organisation and by Jisc, including Acceptable Use Policies, Computing Regulations and Disciplinary Codes. Restrictions imposed by the visited organisations must also be respected. Where Regulations differ, the more restrictive applies;
- Must follow device setup instructions provided by the organisation issuing credentials to maximise confidence that they are connecting to a genuine eduroam service before entering their login credentials;
- Must act immediately on requests by authorised staff of the visited or home organisation that relate to their use of the eduroam service;
- At the end of their association with their home organisation, must remove the eduroam profile from all devices that have been used to connect to the eduroam service and must not attempt to continue to use the service.

Home Organisations

- Must accept the terms and conditions of membership of the eduroam(UK) federation, including user eligibility, which are published on the Jisc Community web site at:
    - https://community.ja.net/library/janet-services-documentation/how-does-organisation-join-service [1]
- Are responsible to the community for the good behaviour of users they authenticate;
- Must enforce this eduroam(UK) Policy in relation to users they authenticate and investigate security breaches affecting their accounts, if appropriate informing any visited organisations that may be affected;
- Must promptly disable, at least with respect to eduroam, accounts of users who no longer have an association with or who have left the organisation;
- Must make their users aware of conditions applying to usage of the roaming service, including Computing Regulations and Acceptable Use Policies;
- Must inform their users about best security practices when using the Service, including how to ensure connection only to genuine eduroam services;
- Must provide support for their users when roaming elsewhere (as a minimum, web-based information must be provided);
- Must provide eduroam(UK) with up-to-date contact details and must act promptly on reasonable requests from eduroam(UK);
- Must inform Janet CSIRT promptly of any apparent breaches of security affecting the privacy of user credentials.

Visited Organisations

- Must accept the terms and conditions of membership of the eduroam(UK) federation which are published on the Jisc Community web site at:
    - https://community.jisc.ac.uk/library/janet-services-documentation/how-do... [2]
- Must ensure that systems that support visiting users are configured, maintained and operated securely, so as not to put the security of other organisations or their users at risk;
- Must make their own AUP readily available to visiting users;
- Must assist Home organisations in supporting their roaming users when required, though the Home organisation will take primary responsibility;
- Must provide visiting users with sufficient information to identify the eduroam services they provide (for example locations covered, service level)
- Must keep sufficient logs to be able to trace provision of eduroam connection/Internet access for an authenticated user?s device (but not necessarily what the specific Internet activity was), including the ?outer identity?, and retain these logs securely for a minimum of three months;
- If activity logs are collected (e.g. on a web proxy), must make the relevant portions available to the Home organisation and/or eduroam(UK) when these are required to investigate misuse;
- Must accept and log complaints of misuse and forward these promptly to the appropriate home organisation;
- Must provide eduroam(UK) with up-to-date contact details and act promptly on reasonable requests from eduroam(UK);
- Must inform Janet CSIRT of any apparent breaches of security affecting the privacy of

user credentials;

- Whilst under no obligation to permit physical access to areas where eduroam Visited services are provided, must only provide Services that are free of charge to users at point of use.

Janet eduroam(UK)

- Must manage the organisational membership of eduroam(UK);
- Must provide the national infrastructure to enable the authentication of roaming users of member organisations to be supported both within the UK and at international participant locations through the Geant eduroam confederation;
- Must provide technical support to member organisations in respect of implementing and operating their eduroam RADIUS services; the scope of such support is described at:
  - https://community.jisc.ac.uk/library/janet-services-documentation/what-t... [3]
- Must protect the security of participating organisations and systems by implementing best practice;
- May exceptionally reduce or remove service without notice when this appears necessary for operational or security reasons;
- Must record authentication attempts and outcome (if possible) and retain these records securely for a minimum of three months and a maximum of twelve months;
- Must provide relevant extracts of this record to the Home organisation or Janet CSIRT when requested to do so;
- Must inform Janet CSIRT promptly of any apparent breaches of security affecting the privacy of user credentials;

Technical Sanctions

As noted below, the design of the Service in the UK gives each party the ability to impose technical controls to protect themselves and the Service against those who represent an immediate threat. However, as the effectiveness of the Service relies on co-operation, such technical measures should be regarded as a temporary solution until the problem can be resolved. Possible technical controls include the following:

- eduroam(UK) may suspend an organisation?s ability to participate in the Service, either as a Home or Visited organisation, for failure to uphold this Policy or the Janet Acceptable Use Policy or the Security Policy;
- Visited organisations may prevent use of their networks by all users from a particular Home organisation by configuring their RADIUS proxy to reject that realm and their access points to re-authenticate users currently connected; in some cases a Visited organisation may also be able to block a single visiting user, but this depends on the particular technology used. In both cases, Visited organisations must inform eduroam(UK) of such measures.
- Home organisations may withdraw an individual user?s ability to use the Service by configuring their own RADIUS server.

If a technical sanction is imposed that affects other organisations this must be reported immediately to eduroam(UK), which will endeavour to assist the organisations concerned to resolve the problem, allowing the full Service to be restored. If a technical sanction involves a particular Home organisation then the Visited organisation should inform that Home organisation as a matter of courtesy.

Links
[1] https://community.ja.net/library/janet-services-documentation/how-does-organisation-join-service
[2] https://community.jisc.ac.uk/library/janet-services-documentation/how-does-organisation-join-service
[3] https://community.jisc.ac.uk/library/janet-services-documentation/what-tech-support-available