

Requirements of an organisation connecting to Janet

6.1 Janet Policies

Any organisation connecting to Janet is required to abide by three policies established to support the role of the network in enabling education and research. These are as follows:

- [Eligibility Policy](#) [1]: states which organisations and people can be given access to Janet;
- [Acceptable Use Policy](#) [2]: states what those people can do on Janet and the responsibilities of their organisations to manage that;
- [Security Policy](#) [3]: states the responsibilities of organisations and Janet to protect the network and other users from security problems.

Each Policy places responsibilities on connected organisations to ensure that its use of Janet does not harm the community with which the network is shared. In extreme cases, persistent failure to respect these policies can lead to a decision to suspend an organisation's connection to the network. Complying with the policies may involve some technical measures, but above all the policies require that every connected organisation has systems and processes in place to encourage proper use of the network, to identify those responsible for any misuse, and to deal with misuse under appropriate disciplinary procedures.

6.2 Legal Requirements

There are also legal requirements on organisations' use of computers and networks. Laws most likely to be relevant to the development of security measures are the [Data Protection Act 1998](#) [4] (processing of personal data) and the [Human Rights](#) [5] and [Regulation of Investigatory Powers](#) [6] Acts (access to content of files and communications). Although there is currently no legal requirement on private networks to retain information about their users, keeping logs to investigate faults and misuse is strongly recommended and a number of [different laws](#) [7] may allow or require these to be disclosed to third parties.

In some circumstances organisations may also be [legally liable](#) [8] for the activities of their members. There is a general principle that an employer will normally be liable for unlawful acts by their employees. For users who are not employees (e.g. students) liability is only likely if the organisation is warned of specific breaches of the law and does nothing to address them; liability for on-line activities may also be excluded if the organisation's only part in the unlawful action was to provide the network connection over which it was carried out.

Our pages of [legal and regulatory information](#) [9] contain more details and links.

6.3 Provision of Filtering Information

Organisations connected to Janet are required to assist in the operation of the network and the investigation of any problems. In particular it is a requirement that all organisations provide, if requested, information to the Janet NOC or Janet CSIRT about any filtering that is used to block access from Janet to particular hosts, networks or services. This will help to prevent waste of network engineers' time in investigating apparent 'faults' which are in fact the result of filtering decisions.

Source URL: <https://community-stg.jisc.ac.uk/library/janet-services-documentation/requirements-organisation-connecting-janet>

Links

[1] <http://community.ja.net/library/janet-policies/eligibility-policy>

[2] <http://community.ja.net/library/acceptable-use-policy>

[3] <https://community.ja.net/library/janet-services-documentation/requirements-organisation-connecting-janet>

[4] <http://www.legislation.gov.uk/ukpga/1998/29/contents>

[5] <http://www.legislation.gov.uk/ukpga/1998/42/contents>

[6] <http://www.legislation.gov.uk/ukpga/2000/23/contents>

[7] <https://www.ja.net/support-advice/advice/legal-regulatory-information/working-law-enforcement>

[8] <https://www.ja.net/support-advice/advice/legal-regulatory-information/regulated-activities/liability-5>

[9] <https://www.ja.net/support-advice/advice/regulatory-legal-information>