Janet Policies and Legal Requirements

Janet manages Janet in accordance with policies set by JISC.

Janet Network Connection Policy

The Janet Network Connection Policy [1] defines explicitly who can connect to Janet.

Primary Connections

All FE and HE organisations and Research Councils are entitled to a Primary Connection to Janet. This type of connection provides access to the full range of network services and support at levels specified in an SLA between JISC and Janet. JISC can also allow other bodies to have a Primary Connection if they are primarily engaged in education or research, or will only use the connection for collaborative research.

Further information about connecting to Janet as a primary site may be found in Section 2 of this manual.

Interconnect Connections

These are available to organisations responsible for the operation of a network, to connect that network to Janet subject to Janet and JISC's agreement. The network will normally be supporting the broader education and/or research community or be delivering educational services to communities that are not directly connected to Janet, such as schools. Interconnect Connections are not subject to the Janet SLA. Only an IP service is normally available - other Janet services are only provided by arrangement.

Further information about Interconnect Connections can be obtained from the Janet Service Desk [2].

Janet Acceptable Use Policy

All organisations connected to Janet are subject to the Janet AUP. This permits Janet to be used for any purpose that is legal, that is socially acceptable to the community Janet serves, and that does not cause degradation of the performance of the network beyond that which might reasonably be expected. All use of the network does, of course, have an impact on performance; the intent is to prevent reckless or inconsiderate activities by members of one organisation causing inconvenience to others.

A key concept of the AUP is that activities, other than those that are detailed below, are

permissible when they are in accordance with the aims and policies of the organisation concerned. An organisation may therefore make its own policy regarding recreational use of Janet by its staff and students, or regarding the use of Janet by departments engaged on external contracts, or by staff engaged upon authorised private consultancy work. Most categories of unacceptable activity are designed to take account of relevant legislation.

Janet may not be used for any of the following:

- the infringement of copyright
- hacking, or other deliberately disruptive activity
- the transmission or creation of obscene or offensive material
- the transmission or creation of material of a threatening nature, or intended to harass, frighten etc
- the transmission or creation of material of a libellous nature
- the transmission of unsolicited commercial or advertising material or similar activities (spamming).

Where advertising material is embedded within, or is otherwise part of a service to which the user has chosen to subscribe, it is deemed to be permissible. Similarly, Janet would be prepared to sanction the use of Janet to transmit obscene or offensive material where this was necessary in pursuance of a properly supervised research project. In these circumstances the organisation must obtain permission from Janet prior to commencing the project, accept responsibility for the legal restrictions that exist and ensure that they are adhered to.

Note that the organisation may be legally liable for serious breaches of these restrictions. Where an organisation is shown to have breached the AUP, JISC may decide to either temporarily suspend the Janet service or withdraw the service for an indefinite period.

A copy of the AUP is sent to each organisation when an initial enquiry is made about the connection process. Additional copies may be obtained from the Janet Service Desk, or the Janet web site at https://community.ja.net/library/acceptable-use-policy [3]

Producing a Local Acceptable Use Policy

All Janet-connected organisations should formulate a local AUP and ask staff and students to sign a declaration to confirm that they will abide by its rules. Students under the age of 18 should have their forms countersigned by their parent or legal guardian.

Suggested Headings for Formulating an AUP

- Introduction (on the need for users to conform to standards of use and behaviour)
- Whom the policy affects
- List of equipment, networks, and data to which the policy refers (i.e. all, but specify items such as 'all servers, PCs, laptops, systems')
- Access to the network(s) (mention use and changing of passwords)
- Viruses and virus checking
- Access to and use of the Internet

- Use of discussion groups and chat (if allowed) (protocols and etiquette should be included)
- Use of software (cover licensing aspects and specify the screensaver software to which users should be limited)
- Copying software (the illegality should be stressed and consequences for students/employees made clear)
- Use of e-mail
- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Copyright, Designs and Patents Act 1988
- Physical security of computing equipment
- Backing-up strategies and rules.
- UCISA publishes model regulations for use of organisational IT facilities and systems at http://www.ucisa.ac.uk/publications/modelregs/modelregs.aspx [4].

Advertising on Janet

There is some limited advertising on the network at present. The formal policy on advertising is set by JISC in the AUP, and Janet is responsible for applying that policy. The Janet Factsheet Advertising describes how this policy is interpreted.

Janet Security Policy

Copies of the Janet Security Policy are available at https://community.ja.net/library/janet-policies/security-policy [5] or from the Janet Service Desk.

Janet is an open network that can be accessed worldwide via the Internet. As such it is subject to security threats from both external and internal sources. Security problems on the Internet or at specific Janet sites can easily spread their impact around the network. Many organisations now rely on the network and connected systems to do their teaching, research and administration. It is therefore increasingly important to protect against security incidents, for example:

- breaches of confidentiality, ranging from intrusion of privacy to theft of intellectual property
- loss of integrity - computers and the information they contain may be modified, casting doubt on the accuracy of the results produced, whether they relate to scientific research or course assessments
- failures of availability, if vital information is lost or destroyed by accident or malice, or if the networks or systems are unavailable due to failure or inappropriate use
- damage to reputation, if intruders boast of their success in attacking the organisation, or use its systems to disseminate unsolicited, unwanted and possibly offensive and/or illegal material
- legal liability, if the organisation is unable to meet its legal obligations as a result of computer failure or misuse.

Each organisation and user connected to Janet is required to comply with the Janet Security

Policy. Organisations with a Primary Connection and others who connect third parties to the network have particular responsibility for the security of both their connection to Janet and that of any Sponsored or Proxy Connections made via their site. They must also ensure that information about security problems can be communicated both within the organisations they provide connections for, and between those organisations and Janet.

All organisations with a Janet connection have a duty to:

- enable users, through training, procedures and systems, to use the network safely
- manage and be accountable for access to Janet by individual users
- manage the risk of insecure network devices and take recommended security measures
- investigate, contain and resolve breaches of security.

All users are required to abide by both Janet-wide policies and those local to their organisation and location, and must cooperate with their organisation and the network operator. In particular, they must follow good security practice and not act in a way that puts the network or connected systems at risk.

The Janet Security Policy recognises that different approaches to security will suit different organisations, and leaves it up to each organisation to choose an appropriate way to meet its obligations under the Policy.

Security Contacts

It is essential that organisations with a Primary Connection have at least one nominated security contact available to provide and receive information on behalf of their organisation. It is accepted that the level of cover will vary depending on the size of the organisation concerned. However, all organisations must accept that, in an emergency, it may become necessary to temporarily disconnect the site if the security contact cannot be reached by Janet CSIRT.

Further information about the Janet Security Policy and advice on setting up a suitable security system for an organisation may be obtained from Janet CSIRT. Section 7 also covers security issues in more detail.

Legal Requirements

The operation and use of networks is subject to various legal requirements. Current information about requirements that are particularly relevant to network and system managers can be found at https://community.ja.net/blogs/regulatory-developments [6]

More general information is available from the JISC Legal Information Service, including a brief guide to IT Law for FE and HE Senior Management. Network and system managers should be familiar with at least the relevant provisions of the following Acts:

Computer Misuse Act 1990

http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm [7]

Data Protection Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980029.htm [8]

Regulation of Investigatory Powers Act 2000

http://www.hmso.gov.uk/acts/acts2000/20000023.htm [9]

Malicious Communications Act 1988

http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm [10]

The Law Relating to Third Party Access to Data

The London InterNet eXchange (LINX®) has published a Best Current Practice document on privacy, which contains useful guidelines on dealing with statutory notices.

Further information about logfiles and third party access to data, including the new RIPA powers, may be found in the Janet Guidance Note on Logfiles.

See also the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000.

JISC Legal Information

http://www.jisclegal.ac.uk/ [11]

Links
[1] http://repository.jisc.ac.uk/7562/1/janet-network-connection-policy-november-2019.pdf
[2] http://www.ja.net/contact-us
[3] https://community.ja.net/library/acceptable-use-policy
[4] http://www.ucisa.ac.uk/publications/modelregs/modelregs.aspx
[5] https://community.ja.net/library/janet-policies/security-policy
[6] https://community.ja.net/blogs/regulatory-developments
[7] http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
[8] http://www.hmso.gov.uk/acts/acts1998/19980029.htm
[9] http://www.hmso.gov.uk/acts/acts2000/20000023.htm
[10] http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm
[11] http://www.jisclegal.ac.uk/