Requirements

Organisations that connect to Janet agree to abide by the Terms for the Provision of the Janet Service, including complying with the Janet Connection, Security and Acceptable Use Policies.2 These Policies exist to support the use of Janet for its intended purpose as the UK's education and research network. The Connection Policy ensures that organisations are only connected to the network where this will benefit that purpose. The Security Policy sets the responsibilities of connected organisations to control the risk of their actions or inactions harming other organisations using Janet or the wider Internet. The Acceptable Use Policy (AUP) defines the types of activity that are permitted (and those not permitted) on the network in order to preserve its research and education purpose, and makes connected organisations responsible for their users' compliance with the AUP.

Janet Policy Requirements for Guests

The Janet Policies make organisations responsible for everyone to whom they grant Janet access, including any guests. In terms of the Security Policy and AUP, guests are no different to the organisation's own users; however three aspects of the Janet Security Policy may require different treatment when an organisation provides Janet access to a guest who does not have a formal link with the organisation, such as someone who is neither their employee nor student. These are contained within sections 6 and 9 of the Security Policy:

> '6. ... Each User Organisation must ensure that all use of Janet by those individuals and Connected Organisations to whom it provides network access complies with this Security Policy and the Janet Acceptable Use Policy. The User Organisation must also ensure that information about security issues can be communicated rapidly within the organisation and to Janet(UK) and that problems are resolved promptly ...'
>
> '9. Each Connected Organisation must act responsibly to protect the network. This duty includes:
>
> - Taking effective measures to ensure that there is no security threat to Janet or other Connected Organisations from insecure devices connected to the Organisation's network;
> - Taking effective measures to protect against security breaches, in particular ensuring that recommended security measures are implemented;
> - Taking effective measures to ensure that security breaches can be investigated and that other users of the network are protected from the consequences of breaches;
> - Assisting in the investigation and repair of any breach of security;
> - Promoting local policies in support of this Janet Security Policy, backed by adequate disciplinary and other procedures for enforcement;
> - Implementing appropriate measures for giving, controlling and accounting for access to Janet, backed by regular assessments of the risks associated with the

measures chosen;
    - Taking reasonable measures to encourage its users to act responsibly in compliance with this Policy and the Janet AUP, and ensuring that they are enabled to do so through systems, procedures and training that support good security practice.'

These mean that the organisation must endeavour:

1. to prevent unauthorised users from gaining access to Janet by using its facilities;
2. to ensure that its provision of Janet access to authorised guests (and, if required, their computers) does not represent a threat to other users of Janet and the Internet;
3. to ensure that authorised guests are informed of, and abide by, the Janet Policies and other policies that may apply to their use of the network connection provided to them.

Methods used to satisfy these requirements for local staff and students may not work for guests. For example, policies and the need to comply with them may be incorporated within staff contracts or student rules, neither of which may cover guests. Protection against unauthorised use may depend on particular configurations of computer and software that cannot be applied (because of licences, permissions, or the time required) to laptops, PDAs or mobile phones brought in by guests.

Approaches that rely on the deterrent effect of possible sanctions, potentially including suspension or dismissal, may be much less effective in controlling the activities of a guest who may not plan to return to the organisation in any case. Organisations offering Janet connections to guests therefore need to plan how they will satisfy these Policy requirements for those guests, and may need to consider different ways of controlling activity from those used for their own staff and students.

Managing Risk

As discussed in the previous section, providing network access to non-members of the organisation represents an increased risk to the organisation. If an organisation provides a person with network access and that access is then used to cause harm to others – whether by hacking, sending malicious messages, downloading illegal material, or many other types of inappropriate use – then the organisation is likely to be blamed. This may in turn cause harm to the organisation, for example (quoting from our factsheet 'User Authentication [1]'):

- ‘The Joint Information Systems Committee (JISC) may, in extreme cases, suspend or withdraw the right to connect to Janet if an organisation’s behaviour represents a serious threat to other users of the network;
- other users may be reluctant to accept communications from an organisation that does not deal promptly and effectively with problem; for example some Janet sites have found themselves on blacklists that prevent them exchanging e-mail with others;
- in a few circumstances, the courts may fine an organisation or imprison its directors if crimes were committed as a result of their negligence, in other words, if they have not taken reasonable care to avoid causing foreseeable harm;
- more often, courts may order organisations to pay damages to individuals or businesses who have suffered loss or harm because of their negligence;
- society and the press may publicly blame an organisation that fails to meet the standards expected of it.’

These risks can never be eliminated without disconnecting entirely from the network; however, it is possible to reduce them to an acceptable level. The Janet Policies (and the Janet community) do not expect connected organisations to remove all possibility of misuse: they expect them to take reasonable care to reduce the opportunities for misuse and to deal with it effectively when it does occur. In deciding whether and how to offer network connectivity to guests, organisations therefore need to balance the benefit they obtain by offering connectivity against the risk that it may cause them harm. As the following sections and case studies will show, there are many different tools and techniques that can be used to reduce the risk of harm. For most organisations, systems for providing guest access will involve the use of a number of these tools and techniques working together to provide an appropriate balance of benefit and risk, with an acceptable level of administrative effort for the organisation. This balance will depend on the circumstances of each individual organisation, including factors such as:

- the number of guests, the duration of their visits, and whether they come from inside or outside the education community
- the degree of connectivity needed by guests, which may be anything from filtered web browsing to high-speed open IP connectivity
- whether access is required in specific locations or generally across the site
- whether guests will use their own equipment or terminals managed by the organisation.

It should also be noted that the organisation’s requirements and assessment of risk may well change over time. Many organisations have found that once they provided a guest facility it has been used in different ways from what was anticipated.

Technological and organisational changes can also change both requirements and risks, as can the expectations of guests. Organisations should therefore be prepared to review their guest access provision and to adapt it to meet new knowledge and requirements. Using a combination of tools, as suggested in this guide, should make it easier for the system to evolve to meet new requirements by adding or modifying components.

Summary

To ensure that an organisation satisfies its responsibilities under the Janet Terms and Conditions, any arrangements made for guest users must provide ways:

- to inform the guest of the AUP and other applicable policies
- to reduce the risk of misuse (including accidental connection of those who are not guests) to an acceptable level. This normally involves both proactive measures to prevent or limit misuse and reactive measures to hold to account those responsible for any misuse that does occur. Clearly the balance between these measures can vary – if the preventive measures are strong there may be less need for control by accountability, and vice versa.

The following sections examine some of the tools that may be used to reduce the risk of misuse, and then give a number of case studies on how different Janet-connected organisations have provided network access for their guests while addressing these issues.

Links
[1] http://community.ja.net/library/advisory-services/user-authentication