Requirements

Document Reference: GEN-DOC-005 - *Please see here [1] for additional document control information.*

Organisations that connect to Janet agree to abide by the Terms for the Provision of the Janet Service, including complying with the Janet network connection, Security and Acceptable Use Policies. These Policies exist to support the use of Janet for its intended purpose as the UK's education and research network. The Janet network connection policy ensures that organisations and individuals 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.

2.1 Janet Policy Requirements for Guests

The Janet Policies make organisations responsible for everyone to whom they grant Janet access, including any guests and visitors. 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. The overall goals of the Security Policy are:

- To ensure that Connected Organisations have appropriate policies and technical controls in place to protect the Janet network, the networks connected to the Janet network and the computer systems and platforms using the Janet network from abuse.
- To ensure that mechanisms exist to aid the prevention and identification of abuse of the Janet network.
- To ensure an effective response to complaints and queries about real or perceived abuses of the Janet network.
-

> To ensure that the reputation of Jisc is protected and that the network can meet its legal and ethical responsibilities regarding its connectivity to the worldwide internet.

These are supported by Responsibilities, which include:

10.2 Each Connected Organisation must ensure that all use of the Janet network by those individuals and Partner Organisations to whom it provides network access complies with this Security Policy and the Janet Acceptable Use Policy. The Connected Organisation must also ensure that information about security issues can be communicated rapidly within the organisation and to Jisc and that problems are resolved promptly.
10.3 Each Connected Organisation and their Partner Organisations must ensure that its actions and those of the users for which it is responsible are safe for themselves and do not present a threat to others.
10.4 Each user of the Janet network and the networks of Connected Organisations and their Partner Organisations must behave in accordance with this Security Policy and with any policies and procedures local to the Connected Organisation. The user must cooperate with their organisation and the network operators to reduce security risks..

Which 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, tablets 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.

2.2 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 [2]'):

- 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 blocklists that prevent them exchanging email 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 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.

2.3 Janet Policy Requirements for Visitors

If Janet is used to backhaul traffic to a public internet access provider for visiting members of the public who are not guests then that traffic remains subject to the Janet Security and Acceptable Use Policies. The Janet network connection policy requires that the traffic must be carried in an encrypted tunnel and that users must be authenticated address part of this requirement, however enforcement of the Policies may require an agreement between the organisation and its partner access provider, especially if the organisation is responsible for the authentication process.

Carrying public traffic in an encrypted tunnel means that any insecure devices that may connect to the public service cannot be used as a way to launch an attack within the Janet network. The use of encryption satisfies Janet's legal duty to protect the privacy of public traffic. If the volume of traffic in the tunnel causes problems for other Janet connected services then Jisc CSIRT are authorised by section 10 of the Janet Security Policy to take such temporary technical measures as may be needed to mitigate those problems until the organisation and its partner access provider are able to resolve them at source.

Requiring authentication means that problems can be traced to an individual account* so that problems can be dealt with at the level of a single user's equipment or behaviour. If this were not done then problems would have to be dealt with by restricting or blocking all public traffic from the organisation. Authentication also satisfies the Janet Security Policy requirement that organisations take appropriate measures to control access to the network, and provides an opportunity to inform users of the policies that apply.

Breaches of the Janet Acceptable Use Policy are likely also to be breaches of the AUP of the partner access provider so the organisation should discuss with the provider how they will be dealt with in accordance with contractual and legal duties. Restrictions applied by commercial providers to accounts or services that are used in breach of policy may differ from the approach normally taken by Jisc.

**Authentication is typically taken to mean authentication of the particular individual accessing the network. Increasingly, options for device authentication are becoming technically available, but these would only fulfil this requirement if an auditable connection to the end user were maintained. For example, if an end user were to be issued with a device that authenticates to the network through its own preinstalled certificate, the organisation would be required to keep a separate record of to whom that device had been issued.*

2.3.1 Legal Issues When Connecting Visitors

As well as the Janet Policy issues, providing network access for visitors (as opposed to guests) is likely to involve additional legal duties. This is because a visitor network is likely to be "available to the public" and therefore classed as a Public Electronic Communications Service (PECS) under Section 151 of the?*Communications Act 2003*?and other laws. *The European Electronic Communications Code (EECC),* which has been implemented in the UK through updates to the *Communications Act 2003*, applies to all electronic communications networks and services, including WiFi networks. The EECC provides a framework for regulation, promoting affordable services, consumer protection measures, and the implementation of very high-capacity networks (VHCNs).

Unlike Janet and most of its customers' networks, providers of Public Electronic Communications Services are subject to additional legal requirements to ensure the integrity of the service, to protect the privacy of users of the network, and to deal in prescribed ways with particular types of misuse. Laws in these areas are developing rapidly, so the following sections can only offer an indicationof where obligations may arise; however organisations offering public access networks need to be prepared to operate these differently from their current networks and, indeed, from some current public access networks.

On privacy the differences are more significant. In order to protect the privacy of traffic on public networks, the interception of communications operations is authorised under the? Investigatory Powers Act 2016 [3]. Warrants authorising interception can only be issued by a Secretary of State, and must be approved by the Investigatory Powers Commissioner's Office.??

Before an interception warrant can be issued, the Secretary of State must believe that a warrant is necessary on certain, limited grounds, and that the interception is proportionate to what is being achieved.? The grounds which would be necessary for interception are: in the interests of national security; the economic well-being of the UK; or in support of the prevention of serious crime.

The Telecoms Directives and their UK transposition also require all privacy breaches on public networks to be reported to the Information Commissioner Office: current guidance is that all breaches must be reported monthly through a breach log, with serious breaches reported immediately. The Commissioner may also require that breaches be reported to affected individuals if the breach is likely to adversely affect the personal data or privacy of subscribers or users. Since encryption is considered an acceptable way to mitigate damage from any privacy breaches organisations offering visitor access should ensure that wherever possible this traffic is encrypted and that the operation of networks and equipment carrying it meets the standards required by the Act and Directives.

Governments are increasingly viewing network providers as key partners in managing threats both to and from users of the Internet. In some areas this has already been formalised in legislation: the?*Data Retention and Investigatory Powers Act 2014*??required public networks to retain information about when users logged on, who they emailed and telephoned. This has since been replaced with the *Data Retention and Acquisition Regulations 2018* which introduced a code of practice called “Communications Data” setting out rules for retaining any data. It provides that telecoms operators must comply with data protection legislation (where the data constitutes personal data). The?*Digital Economy Act 2017* ?may require them to block access to adult sites that do not implement age verification. Following this, the Government published a draft Online Safety Bill in May 2021 to introduce a new online harms framework, however, the House of Lords Communications and Digital Committee deemed the draft bill “inadequate” for protecting children from harm. With regards to this, the Government stated it would “use the pre-legislative scrutiny process to explore whether further measures to protect children are required”. Most of these duties require the ability to distinguish individual users, so are most naturally done by the organisation that manages accounts and authenticates users. Where a public communications service is provided by collaborating organisations, for example where one provides wireless infrastructure and another does user account management,?laws normally?allow the organisations to agree which of them will perform the duties required. Organisations providing public access should therefore agree the division of these legal duties – and any that may arise in future – with their partner internet access provider.

Although no law has yet mandated that all public Internet access must be authenticated, these and similar laws are likely to cause difficulties for unauthenticated networks since without control of individual users there may be no way to deal with a problem other than to turn off the entire service.

2.4 Summary

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

a) to inform the guest or visitor of the AUP and other applicable policies

b) to reduce the risk of misuse (including accidental connection to Janet 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 section provides some case studies on how different Janet-connected organisations have provided network access for their guests and visitors while addressing these issues.

Links
[1] https://community.ja.net/library/janet-policies/network-access-guests-technical-guide
[2] https://community.ja.net/library/janet-policies/user-authentication
[3] https://www.gov.uk/government/collections/investigatory-powers-bill