



Welsh Networking Ltd
RHWYDWEITHIO CYMRU CYF

Connection, Security and Acceptable Use Policy

v1.0 13 August 2002



WNL CONNECTION, ACCEPTABLE USE & SECURITY POLICY

This document details the Welsh Network Limited Connection Policy, defining the conditions under which organisations are eligible for connection to the South Wales MAN, the Acceptable Use that the connection may be used for, and the Security responsibilities of that organisation whilst connected to the SWMAN. It forms an integral part of the Network Services Agreement that is entered into between a connected organisation and Welsh Network Limited.

1. BACKGROUND

- 1.1 Welsh Networking Limited has been established to:
- Provide a regional high bandwidth network, the SWMAN, supporting collaboration between institutions for learning, teaching and research, using existing and emerging networked applications;
 - Provide a resilient high bandwidth network route from the SWMAN to JANET (the Joint Academic NETwork) and the global Internet;
 - Provide a nucleus for a future regional broadband network, connecting other public sector organisations such as educational institutions, museums, libraries, local authorities, and private sector enterprises, and acting as a regional resource supporting the work of the National Assembly for Wales.
- 1.2 The bandwidth available within the SWMAN and particularly at the point where the SWMAN interconnects with JANET is a valuable but limited resource. Access to the network will need to be justified, authorised and funded, the usage of the network will need to be lawful and proper, and the network itself made secure and protected against misuse. These elements of SWMAN access and usage are addressed by the WNL Connections Policy, Acceptable Use Policy and Security Policy detailed here, and by the associated Charging Policy.
- 1.3 Within these practical restraints, extending the effective coverage of the SWMAN to other organisations is a desirable objective. Welsh Networking Limited will therefore seek to offer connections to the SWMAN in as open and easy a manner as possible subject to connection policies that protect itself, its members and its customers for practical and legal purposes.

2. ACCESS TO JANET AND THE INTERNET

- 2.1 JANET (the Joint Academic NETwork) is the high bandwidth UK national network funded by, and for, the Higher Education, Further Education and Research communities. JANET is managed by the not-for-profit company UKERNA (UK Educational and Research Network Association).

2.2 Connection to the SWMAN does not in itself entitle an organisation to access JANET and the Internet although there is recognition that most organisations will wish to do so. Organisations wishing to access JANET via the SWMAN will need to obtain appropriate authorisation and will be subject to the regulations and associated charges that are determined by UKERNA/JISC.

2.3 As local and regional partnerships between education and private sector enterprises evolve it is anticipated that industrial and commercial partners will seek Internet access via an educational institution and/or via the SWMAN. In these circumstances WNL will route Internet traffic via JANET or a commercial Internet Service Provider as appropriate.

3. WNL CONNECTION POLICY

3.1 Classes and Types of Connection

3.1.1. A **User Organisation** is any organisation that is connected to the SWMAN (directly or indirectly) for the provision of an agreed schedule of networked services. Two main **classes** of connections are defined for User Organisations:

3.1.2. **Nominated Connection** – is a connection to the SWMAN that has been requested by UKERNA/JISC, and the funding for which is via UKERNA/JISC. The User Organisation will have a contractual agreement with UKERNA for the provision of JANET Services, including Internet access.

3.1.3. **Local Connection** - is a connection to the SWMAN that has been requested by the user organisation itself, and the funding for which is from that organisation. The contractual agreement for provision of networked services is between the User Organisation and Welsh Networking Limited. Internet access may be via JANET or a commercial Internet Service Provider, as appropriate to the type of organisation.

3.1.4. Nominated and Local Connections may be further classified into three **types** of connection – **Primary, Sponsored** or **Proxy**.

3.2 Primary Connection

3.2.1. A Primary connection is a direct connection provided by the SWMAN, and which provides access to the full range of services and support specified in the Network Services Schedule and Service Level Agreement (SLA) Schedule of the Network Services Agreement. User organisations in receipt of Nominated Connections also benefit from the services and support offered by UKERNA under a separate SLA between UKERNA and the JISC.

3.2.2. All Higher Education Institutions and Further Education Colleges hold Primary connections to the SWMAN. Research Council sites



are entitled to primary connections. Other organisations are allowed Primary connections if they are primarily engaged in education or research, or will only use their connection for collaborative research.

3.2.3. A primary connection is normally to the SWMAN core network. The connected organisation would provide its own Domain Name Service (DNS), Web service and email service and would have direct network access to the Internet via the SWMAN.

3.3 Sponsored Connection

3.3.1. An organisation with a primary connection may provide a sponsored connection to the SWMAN for a third party network. This scheme permits the primary site to 'sell' part of its bandwidth to the site they have agreed to host. These arrangements are normally made between organisations with a close working relationship and where the activities of the third party are primarily to support the teaching, learning and research aims of the host organisation.

3.3.2. A sponsored connection is normally to equipment at a primary connected site, but exceptionally it could be to the SWMAN backbone itself. The sponsored organisation would be expected to provide its own Domain Name Service (DNS), Web service and email service and would have direct network access to the Internet via the SWMAN.

3.3.3. There are a number of aspects that distinguish a Sponsored Connection from a Primary Connection:

- the management and support of a Sponsored Connection, and any associated service levels, are a matter for agreement between the sponsoring organisation and the third-party sponsored organisation being connected;
- the provision of such a connection implies that the sponsoring organisation, as host, assumes the responsibility to ensure that users within the third-party organisation are aware of the WNL Acceptable Use Policy (AUP), and it must have mechanisms in place to deal with failure of the third party to abide by this policy.
- a sponsored organisation cannot onward sell a sponsored connection to another organisation, although it may offer proxy services subject to the agreement of the primary hosting organisation and WNL.
- it is the responsibility of the sponsoring primary site to ensure that the sponsored site does not use excessive bandwidth.



- 3.3.4. Payment for a sponsored connection is annually to the hosting site. This payment will include maintenance and service elements, a UKERNA license fee and a WNL fee. There may also be an initial physical connection charge to cover any additional cabling and equipment connectivity at the sponsoring site, and a charge relating to JANET network usage.
- 3.3.5. Applications to add a sponsored connection will be submitted by a primary site to a panel of the WNL Management Committee who will report to the WNL Board the connections that have been approved. Applications that meet the Purpose of WNL as defined in the Consortium Agreement will not be unreasonably refused.
- 3.3.6. At the present time (June 2002) the status of sponsored connections is under review by the JISC and UKERNA, in consultation with representatives from the UK Regional MANs community.

3.4 Proxy Connection

- 3.4.1. A Proxy connection is an indirect connection for a third party who does not otherwise have authority to connect to the SWMAN or JANET. The third party may be an individual user, small group or organisation.
- 3.4.2. The primary or sponsored organisation hosts network services (e.g. email, web pages) for the third party, and the third party would gain access to the Internet via the hosting site services.
- 3.4.3. The host organisation is responsible for all support of the beneficiary user/organisation.
- 3.4.4. A proxy connection cannot onward sell proxy services.
- 3.4.5. Payment for proxy services is annually to the hosting site. This payment will include a maintenance element, a service element (e.g. to cover the cost of providing web hosting) and an amount to defray any UKERNA or WNL proxy license fees. There may also be an initial physical connection charge to cover any additional cabling and equipment connectivity at the hosting site, and a charge relating to JANET network usage.

3.5 User Organisation Responsibilities

- 3.5.1. A User Organization with a primary, sponsored or proxy connection agrees to be bound by the agreement it enters into with WNL. Furthermore, this becomes explicitly part of the organisation's agreement with its own user community.
- 3.5.2. WNL will hold a register of all connected organisations. This will list the connected organisation and the hosting organisation. Maintaining this register and policing the use of these



connections is the responsibility of the organisation hosting the connection.

4. WNL ACCEPTABLE USE POLICY

4.1 Background and Definitions

4.1.1. This Policy applies to any organisation authorised to use Welsh Networking Limited's SWMAN network and WNL's network services (a User Organisation). It is the responsibility of the User Organisation to ensure that members of their own user communities use WNL's network and services in an acceptable manner and in accordance with current legislation.

4.2 Acceptable Use

4.2.1. A User Organisation may use the SWMAN for the purpose of interworking with other User Organisations, and with organisations attached to networks that are reachable via interworking agreements operated by WNL. All use of the SWMAN and WNL's services is subject to payment of the appropriate charges in force during the period of service. Any provision of service must be authorised in advance.

4.2.2. Only Primary, Sponsored, Proxy or other authorised connections may use the Joint Academic Network (JANET) to which the SWMAN is connected. Only those contracted to do so may use any other Internet feed that is accessible via the SWMAN.

4.2.3. Subject to the following paragraphs, the SWMAN may be used for any lawful activity that is in furtherance of the aims and policies of the User Organisation.

4.3 Unacceptable Use

The SWMAN may not be used for any unlawful or unacceptable purposes, which include but are not confined to:

- the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- the creation or transmission of defamatory material;
- the transmission of material such that this infringes the copyright of another person;
- the transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks, save where that material is



embedded within, or is otherwise part of, a service to which the member of the User Organisation has chosen to subscribe;

- deliberate unauthorised access to facilities or services accessible via the SWMAN;
- deliberate activities with any of the following characteristics:
 - wasting staff effort or networked resources, including time on end systems accessible via the SWMAN and the effort of staff involved in the support of those systems;
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - continuing to use an item of networking software or hardware after WNL or their Managing Agent has requested that use cease because it is causing disruption to the correct functioning of the network;
 - other misuse of SWMAN or networked resources, such as the introduction of "viruses";
- any action which prevents WNL from maintaining the SWMAN;

4.4 Where the SWMAN is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the SWMAN. In particular, where a user organisation is authorised to access the JANET network via the SWMAN, the JANET Acceptable Use Policy will apply and will assume primacy over the WNL AUP.

4.5 Passing on and Resale of Welsh Networking Service

4.5.1. A User Organisation is not permitted to provide access to the SWMAN to third parties or to permit traffic from a third party to be carried over the SWMAN without the prior agreement of Welsh Networking Ltd, except to extend access to others on a limited basis. For example, it is acceptable that a visitor to the User Organisation be permitted to gain access to the network for the purpose of maintaining contact with his or her home organisation. It is intended that such use be regulated by the User Organisation in the same manner as it would regulate occasional use by third parties of its other facilities, such as its telephone and IT support systems.

4.5.2. A third party, where it applies to an individual, means someone who is not acting as a member of the User Organisation. Where



it applies to a separate organisation, this is defined to be any organisation that is in law a separate entity to the User Organisation.

4.6 Compliance

- 4.6.1. It is the responsibility of the User Organisation to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the network does not occur. The discharge of this responsibility must include informing those at the Organisation with access to WNL's network of their obligations in this respect.
- 4.6.2. If a User Organisation is in violation of these conditions of use, where necessary, service may be suspended or withdrawn from the User Organisation. Such action would not normally be taken without prior discussion with the User Organisation.
- 4.6.3. However, where a violation causes serious degradation of the service to other users of the SWMAN or JANET, suspension may be made on the judgement SWMAN Managing Agent, WNL or UKERNA, and service would only be restored when the cause of the degradation of service to others had been removed.
- 4.6.4. Should a violation of these conditions persist after WNL or its Managing Agent has given appropriate warnings, the service may be withdrawn indefinitely. Such a withdrawal of service would only be made on the authority of the WNL. Restoration would be made only when WNL was satisfied that the appropriate steps had been taken at the Organisation involved to ensure acceptable behaviour in future.
- 4.6.5. Where violation of these conditions is illegal or unlawful, or results in loss or damage to Welsh Networking Ltd resources or the resources of third parties accessible via the SWMAN, the matter may be referred for legal action.
- 4.6.6. It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of SWMAN resources on the part of users and appropriate disciplinary measures taken by their Organisations.

5. WNL SECURITY POLICY

5.1 Purpose of a Security Policy

- 5.1.1. The SWMAN (and the User organisations' networks connected to it) form part of the UK JANET network and the global Internet. The assumption is made that any device authorised to be connected to the user organisations' network and onward to the SWMAN and JANET may exchange data with any other such site(s).



- 5.1.2. These principles of access are inherent in the use made of the network by the academic community, and in the software that it uses across that network.
- 5.1.3. However, the laws now relating to Internet use require organisations (user organisations and regional network operators) to be aware of their responsibilities and to take appropriate action to minimise their legal risk and liability. Laws relating to Internet use include the Data Protection Act, the Defamation Act, Copyright Law, the Obscene Publications Act and the Computer Misuse Act.
- 5.1.4. Any imposed system of general access control and/or monitoring of use may cause extreme difficulty for users, and might in any case be technically impossible. Core network equipment must however be protected with appropriate access controls and access to this equipment must be under the direction of WNL's Managing Agent.
- 5.1.5. Clearly, such an open global network presents some dangers. Among the threats which exist are:
 - Breaches of confidentiality, ranging from intrusion of privacy to theft of intellectual property
 - Dissemination of unsolicited and unwanted, and possibly offensive and/or illegal material
 - Destruction of information and/or temporary disabling of remote systems
 - Misuse of the publicly funded resource for purposes which do not benefit the community and may be illegal in themselves
- 5.1.6. From the point of view of the connected user organisation, such threats may arise either externally or internally.
- 5.1.7. In providing a network with open access, the assumption is made that these dangers can be contained by responsible action by all the connected organisations and their user communities. In particular, organisations and their users must adhere to the WNL Acceptable Use Policy and, where appropriate, the JANET Acceptable Use Policy.
- 5.1.8. The freedom of network use entails that the connected organisations and their network users accept the duty to take all proper precautions to enforce adequate access control, in order to deter and, as far as possible, prevent misuse by others. This duty is essential, because failure by one site to act responsibly may have implications for other sites or even for the whole network.



5.1.9. In the context of the global network, this duty may be defined in terms of a cascade. The operator of any network that connects to any other network must assume responsibility for performing the duty. However, the operator may perform the duty by ensuring that every user performs this duty fully in respect of his/her connection to the network, so that the sum of the actions by all users is effective security for the network.

5.1.10. Such a method of achieving security demands that any organisation which is required by WNL to exercise a duty of providing adequate security, and of controlling the actions of its own users, must be fully aware of the duty, of the risks, and of the resources available to assist with the task.

5.2 Site Agreements

In order that connected sites are fully aware of the duties that fall to them, and of the consequences of failure to carry out those duties, it is essential that a written and binding Network Services Agreement exists between WNL and all SWMAN primary sites. The primary site is equally responsible for actions by sponsored and proxy users connected through their site to SWMAN, and should put in place similar subsidiary agreements to protect it.

5.3 Points of Contact

5.3.1. Where any such cascaded responsibility exists, it is essential to identify individual points of contact within connected organisations. These nominated points of contact need to be available to provide and receive information on behalf of the organisation, and they need to be able to do so throughout any period for which the organisation is carrying this responsibility.

5.3.2. For a number of SWMAN sites operating as Points of Presence, this will mean extended periods of cover, and these sites need to have an accessible central contact throughout the whole of the same period.

5.3.3. At other connected sites, such cover may not be appropriate. However all sites must accept that, in an emergency, if the central point of contact is unable to reach the nominated site contact, it may become necessary to disconnect the site until the situation at the site is brought under control.

5.3.4. All connected organisations are required to provide nominated site contacts, and must keep WNL informed about that contact.

5.3.5. The SWMAN Managing Agent provides and manages the central contacts for the SWMAN Points of Presence.

5.4 Responsible Action by Sites



5.4.1. WNL requires users and organisations to act responsibly. In respect of organisations, this duty includes:

- encouraging users to act responsibly, and ensuring that they are enabled to do so
- exercising responsibility about giving and controlling access to the SWMAN and JANET
- taking measures to protect against attack
- providing adequate disciplinary and other procedures to enforce an appropriate local policy
- assisting in the investigation of a breach of security

5.4.2. The JANET-CERT provides JANET users with accurate and comprehensive information and support on a range of security topics. WNL expects connected organisations and the SWMAN Managing Agent to:

- maintain awareness of JISC security policy and advice
- maintain awareness of current perceived threats reported in the UK or elsewhere, and recommended means of addressing them
- maintain awareness of recommended general security tools and implementing them as appropriate

5.4.3. The aim is that all relevant sections of the SWMAN community should be aware of the potential threats to their own and other institutions, and of the actions they are responsible for taking to thwart them.

5.5 Monitoring and Enforcement

5.5.1. It follows from the principle of cascaded responsibility backed up by the Network Services Agreement and the Acceptable Use Policy, that there must be some method for WNL to enforce the possible disconnection of a user organisation, and to provide full access and assistance to law enforcement agencies where necessary.

5.5.2. WNL reserve the right to monitor use of the network to ensure the integrity of the SWMAN and also to ensure compliance with relevant Internet use legislation.

5.5.3. WNL therefore assumes the responsibility (in conjunction with the SWMAN Managing Agent) to

- Monitor use of the network, as far as is possible while respecting privacy, either in response to information about a specific threat, or generally because of a perceived situation
- Require a primary connected site, through its nominated contact, to rectify any omission in its duty of responsibility



- Where a site is unable or unwilling to co-operate, to initiate the procedure for achieving an emergency disconnection
- Obtain evidence and pass on information as necessary in order to assist an investigation by a law enforcement agency
- Provide support and co-ordination for investigations into breaches of security