

Northern Grid for Learning Acceptable Use Policy

This Acceptable Use Policy refers to the regional broadband network supplied by Northern Grid for Learning to schools and Local Authority establishments. This policy explains the behaviours, which are acceptable and unacceptable with regard to usage of the regional broadband service.

Any school, LA or other educational organisation using Northern Grid for Learning's Network or Service is required to comply with this Acceptable Use Policy (AUP). Failure or non-compliance may result in the school's broadband service being disconnected.

This Acceptable Use Policy has been endorsed and approved by the Northern Grid Board of Directors who are all senior managers within partner Local Authorities.

Northern Grid for Learning's vision is to support schools and Local Authorities to use creatively and safely a wide range of innovative and integrated broadband technologies. The company seeks to promote high standards of teaching and learning by supporting the effective use of ICT.

This policy applies to all users of the Northern Grid broadband network whether in school or Local Authority offices. This includes local authority officers, head teachers, governors, teachers, pupils, classroom assistants, parent or voluntary helpers, school caretakers and other ancillary staff.

All users should note that the Northern Grid broadband network is monitored on a regular basis. Any user who is found to deliberately infringe this policy may be subject to disciplinary procedures or legal action.

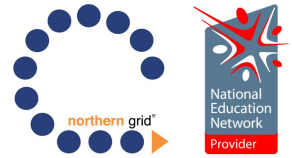
The Northern Grid Network and Services are provided to you by Northern Grid for Learning, a company registered in England and Wales (company number 4824016) whose registered office is 11 Vance Business Park, Norwood Road, Gateshead, NE11 9NE.

Unlawful and Illegal Use

All material, which depicts the abuse of children and young people, is illegal. Other illegal material includes race hatred, incitement to violence. These are not exclusive categories. There may be other information that is deemed to be illegal.

Accidental access to material, which may be classed as illegal should be reported to the Internet Watch Foundation – www.iwf.org.uk.

If you receive images or content including sound files, which you believe could be illegal it is imperative that you make no attempt to investigate the content. A log reference should be made to show that there is suspicion of inappropriate or illegal material. This log reference is to protect you from any suspicion for having potential illegal material in your possession. Once this log has been made the URL if appropriate should be reported to the Internet Watch Foundation – www.iwf.org.uk. This must be done by typing the URL address into the report not by copy and paste. It is possible to accidentally open a link so care must be taken.



If the content is an image in the body of an email close the email and make a log reference. A report should be made to the IWF. They will advise what to do next. **Under no circumstances forward the email, copy the image or show it to another person, as each of these actions constitutes an illegal offence.** The IWF, is licensed to investigate, you are not.

The Northern Grid Wide Area Network (WAN) and associated services may be used for lawful purposes only.

As a user of this Service you agree not to use the Service to send or receive materials or data, which is:

- in violation of any law or regulation
- which is defamatory, offensive, abusive, indecent, obscene
- which constitutes harassment
- is in breach of confidence, privacy, trade secrets
- is in breach of any third party Intellectual Property rights (including copyright)
- is in breach of any other rights or has any fraudulent purpose of effect.

You are prohibited from storing, distributing, transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of, any unlawful material through the Service.

Examples of unlawful material include:

- Direct threats of physical harm
- Child abuse images
- Incitement to racial hatred
- Copyrighted, trademarked and other proprietary material used without proper authorisation

You may not post, upload or otherwise distribute or permit the posting, uploading or distribution (whether intentionally or otherwise) of copyrighted material on our servers without the consent of the copyright holder.

In the event Northern Grid or Easynet becomes aware of any breach of this clause, Northern Grid or Easynet may take action. The storage, distribution, or transmission of unlawful materials could also lead to UK authorities alleging criminal liability.

Inappropriate Use

Inappropriate use of the network includes accessing or having possession of material that is thought to be offensive such as, adult pornography of any level, content of an obscene, indecent and/or abusive nature. **You should be aware that disciplinary and/or civil action might arise if users are found to be accessing material of this nature across the school, Local Authority or regional network.**

Violations of system or network security

Any violations of systems or network security are prohibited, and may result in the user facing criminal and civil action. Northern Grid will investigate incidents involving such violations and will

inform and co-operate with the relevant law enforcement organisations if a criminal violation is suspected. Violations may include, but are not limited to, the following:

- Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network
- Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network
- Interfering with any user, host or network including mailbombing, flooding, and deliberate attempts to overload a system and broadcast attacks.

All machines connected to the Northern Grid network must have full up to date and appropriate anti virus and anti spam protection.

Any machine found to be infecting the Local Area Network (LAN) must be immediately disconnected, cleaned and not reconnected to the LAN until fully checked by an authorised school officer.

Northern Grid will request that Easynet disconnect from the WAN, any site that fails to comply with this procedure. No site will be allowed to disrupt or infect the WAN thereby having a detrimental effect on all other users.

Network Usage

Sites must not connect to the network any unprotected machine, insecure proxy servers, or other machines vulnerable to unauthorised remote access giving unknown attackers access at either user or administrator level.

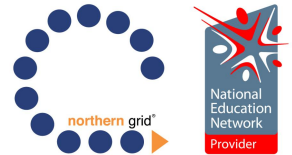
Caches that have been purchased by LA sites and schools through Northern Grid are delivered with a default setting which blocks inappropriate sites. Any LA site or school that alters the default settings may not be using a system that meets Becta accreditation.

No LA, school or organisation connected to the Northern Grid WAN is permitted to distribute bandwidth beyond the school or site building without first requesting permission. An example of this would include creating an external wireless network to deliver broadband to another external site. Permission will only be given if Northern Grid is satisfied that all safety and security measures have been put in place and that such transmissions do not have a detrimental effect on the functionality of the regional network.

The regional network has the capability of delivering voice over IP telephony. However the current configuration does not enable this functionality. Any user wishing to implement VoIP must first contact Northern Grid. Permission will only be given if Northern Grid is satisfied that all safety and security measures have been put in place and that such transmissions do not have a detrimental effect on the functionality of the regional network.

Security and Protection

All users of the regional broadband network are required to be individually identifiable. This means that every user of the network must have an individual username and password. This must be securely kept and not passed onto other users. **In the event of an investigation into misuse, proper use of passwords will protect innocent users from the upset and embarrassment of suspicion for inappropriate or illegal misuse.**



Those members of staff who have administration rights to their school network should take care to ensure that no unauthorised user obtains access to their admin password. This includes accidental or deliberate access by leaving admin machines active when not in use by authorised personnel.

Email Use

You may not send e-mail to any user who does not wish to receive it. Northern Grid recognises that e-mail is an informal medium. However, users must refrain from sending further e-mail to a user after receiving a request to stop. Chain letters are unsolicited by definition and may not be propagated using the Service.

Flood emails will result in the site's broadband connection being shutdown.

You may not send, distribute, or reply to mailbombs. Mailbombing is defined as either e-mailing copies of a single message to many users, or sending large or multiple files or messages to a single user with malicious intent.

You may not use false email headers or alter the headers of e-mail messages to conceal their e-mail address or to prevent Internet users from responding to messages. You may not use any email address that you are not authorised to use. [Private email addresses are not advised for formal educational business. This is to provide a level of protection and privacy for individual members of staff.](#)

Violations of the AUP outlined in this document can sometimes result in massive numbers of e-mail responses. If Users receive so much e-mail that the Northern Grid WAN or any associated service is affected, we will request Easynet to shut down that User's account.

Advertising to Unsolicited Email Recipients

You may not operate, host, provide hosting facilities to or assist in any way whatsoever any web site, email address, email service, ftp service or any other online service, which is advertised or promoted by means of Unsolicited Bulk Email.

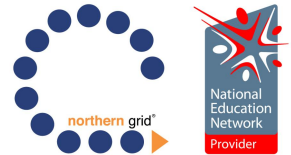
World wide web usage

[All school machines, which are connected to the regional broadband network, should access the Internet via the Equinet CachePilot or other secure proxy server device. Failure to do this may result in unfiltered Internet access being available and may lead to the ICT manager of the school facing investigation into inappropriate use.](#)

[Northern Grid and Easynet provide filtering via SmartFilter and where purchased, Equinet Cachepilot. The regional broadband service complies with banned sites listed by the Internet Watch Foundation. Attempts to access these banned sites may result in the user being reported to the appropriate authorities resulting in legal or civil actions.](#)

The laws of all nation states, regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax, apply equally to on-line activities. However, the practical legal position regarding Internet usage is often uncertain.

Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion,



national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Strictly, material must not be accessed from the web, which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.

Given the impracticality of assessing the exact legal position with regard to the previous two paragraphs, Northern Grid's acceptable use protocol governing material that could be objectionable on the above grounds, is grounded in English law.

Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.

From time to time, Internet usage from the Northern Grid network is monitored and a log is kept of all sites visited. Any violations identified may result in further investigation and potential criminal/disciplinary action. Where authorised by a LA Northern Grid will proactively monitor, log and investigate Internet access for an entire site or nominated users. Reporting on aggregate usage is performed on a regular basis.

Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Such files must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

Relevant legislation

The following are a list of Acts that apply to the use of Northern Grid Network and Services:

- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Data Protection Act 1998
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights

Use of Mobile Devices

Northern Grid for Learning does not prohibit the use of mobile devices on the regional network. However, users should note the following items. These examples are for clarification. They are not exclusive.

1. Any mobile device must be checked for viruses and spam content before being attached to the regional broadband network.
2. Mobile devices must not be used to take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission.
3. Any use of mobile technology to intimidate, bully, harass or threaten others will be counted as an infringement of network use. This may result in disconnection from the network or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission.
4. Any images that involve children must not identify children by name and permission must have been agreed by the subject and/or relevant parent / carer before posting. A record should be made of who will be taking the photos, why the photos are being taken, when they are being taken and what they are to be used for. This should all be documented in the risk assessment carried out before a school trip or event. The photos should then be stored in a safe area within the school LAN and only used for legitimate educational purposes as directed by the Headteacher.

Use of Video Conferencing Across the Regional Network

The regional broadband network facilitates effective video conferencing. As an educational tool, this system has many benefits. However, to ensure effective safety, schools are recommended to use the following:

1. Always book the VC session via the national JVCS booking system. This ensures that you will be connected to the correct end user and that the session is monitored.
2. Always use VC in a public place. Do not leave pupils or young people unattended during a live VC event.
3. Report any misuse of VC to your school E-Safety officer and to the Northern Grid for Learning.

Reporting Accidental Access to Inappropriate Material

Like any online service, it is impossible to guarantee that there will never be accidental access to inappropriate or offensive material.

Any user of the Northern Grid network who accidentally comes across inappropriate or offensive material should do the following:

1. Inform the school's E-Safety officer of the incident and give the website address.

2. Ask the E-Safety officer to log the web address, time and username in the school web log book.
3. If Easynet decide that the website is not sufficiently inappropriate for permanent blocking, the school should block the website via its own CachePilot or other proxy server.

Reporting Accidental Access to Illegal Material

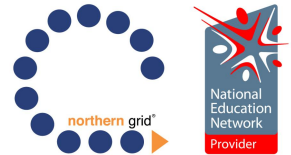
Any User of the Northern Grid Network who accidentally comes across illegal material should do the following:

1. Report the incident to the Headteacher or senior manager
2. Do not show anyone the content or make public the URL
3. Make sure a reference is made of the incident in a log-book
4. Go to the IWF website at www.iwf.gov.uk and click the report button
5. If reporting a URL do not use copy and paste, type the URL

Reporting Suspected Deliberate Abuse or Misuse

Any person suspecting another of deliberate misuse or abuse of the regional broadband network should take the following action:

1. Report in confidence to the school E-Safety officer or headteacher of the school.
2. The headteacher should inform the Local Authority.
3. The Local Authority should complete an internal RIPA form, requiring Northern Grid to complete an internal investigation.
4. If this investigation results in confirmation of access to illegal materials or the committing of illegal acts, Northern Grid will inform the relevant police authority who will complete their own investigations.
5. If the investigation confirms that inappropriate behaviour has occurred, Northern Grid will inform the relevant authority. This may be the Local Authority or the School's Board of Governors.
6. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.



Examples of Inappropriate Use:

- Visiting pornographic sites (adult top shelf materials)
- Causing offence to religious groups
- Inappropriate use of email
- Deliberate sabotage of the network; i.e. hacking, mail bombing etc.

Access to Illegal Material

If this investigation results in confirmation of access to illegal materials or the committing of illegal acts, Northern Grid or Easynet will inform the relevant police authority that will complete their own investigations and a criminal investigation may follow.

Examples of Illegal Acts:

- Accessing any child abuse images.
- Incitement to racial hatred
- Incitement to violence
- Software media counterfeiting or illegitimate distribution of copied software.

Decision to Advise the Police for Criminal Investigation

On the facts that are immediately available, a decision will be taken whether to refer the matter to the Police for criminal investigation. This does not preclude the matter being referred to the Police at any later stage when a formal investigation has been undertaken.

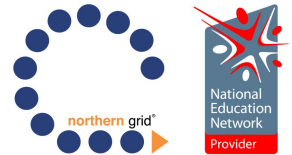
Where Northern Grid are approached by an officer in an LA or any public body and asked to provide evidence or monitoring of a suspected site the following rules will apply.

The Regulation of Investigatory Powers Act 2000 and its Application for Northern Grid

The Home Office states that:

“The Regulation of Investigatory Powers Act 2000 (RIPA) provides for, and regulates the use of, a range of investigative powers, by a variety of public authorities. It updates the law on the interception of communications to take account of technological change such as the growth of the Internet. It also puts other intrusive investigative techniques on a statutory footing for the very first time; provides new powers to help combat the threat posed by rising criminal use of strong encryption; and ensures that there is independent judicial oversight of the powers in the Act.”

Each police force and most councils including the members of Northern Grid are defined as a Public Authority to which RIPA applies. The forms of surveillance that the police and any council are entitled to authorise are covert directed surveillance and the use of covert human intelligence sources (informants). In any council only officers of the rank of deputy chief officer and above may be designated as Authorising Officers under RIPA. No covert directed surveillance or use of covert human intelligence sources may be undertaken without obtaining authority from such an Authorising Officer.



RIPA requires that third parties (Northern Grid), that are required to provide information about other people subject to surveillance and investigation, should be approached for that information in a highly controlled manner by means of standard forms published by the Home Office.

Northern Grid will require that all such applications for information be made in the appropriate manner.

Disclaimer

Northern Grid and Easynet will endeavour, wherever possible, to provide a safe and secure environment for its users. However, users must be aware that we cannot guarantee complete safety from inappropriate or illegal material.

For further details of Easynet's AUP please go to:

<http://www.uk.easynet.net/legal/acceptable.asp>