

## Acceptable Use Policy 2011 - Executive Summary

The Northern Grid Wide Area Network (WAN) and associated services may be used for lawful purposes only. You are prohibited from storing, distributing, transmitting or permitting the storage, distribution or transmission (whether intentionally or otherwise) of any unlawful material.

Find the full version of this Acceptable Use Policy at [www.northerngrid.org/aup](http://www.northerngrid.org/aup)

### Enforceable

checkbox

#### Inappropriate Use

Accessing or having possession of offensive material such as, adult pornography of any level, content of an obscene, indecent and/or abusive nature could result in a disciplinary and/or civil action.

#### Monitoring and Reporting

The Northern Grid network is monitored. Logs may be kept of sites visited. Any violations identified may result in further investigation and criminal/disciplinary action.

#### Violations of system or network security

Machines and organisations will be disconnected if security is violated.

Machines connected to the Northern Grid network must access the internet through an approved security / web filtering appliance.

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

#### Network Usage

Unprotected devices must not be connected to the network. Unprotected remote access is not permitted.

All workstations and servers must be hardened; the school must have a patch management policy for OS and application upgrades.

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 from Northern Grid.



## Identification of Users

All users of the Northern Grid network, including remote users, are required to have individual user names and passwords.



## Use of Video Conferencing

All VC endpoints making and receiving calls must be registered with the NG Gatekeeper.



## Email Use

You may not send email to any user who does not wish to receive it.

You may not use false email headers or alter the headers of e-mail messages to conceal their email address or to prevent Internet users from responding to messages. You may not use any email address that you are not authorised to use.

Email or other attacks which flood the network are prohibited. If these occur, the originator will be disconnected from the NG network.

You may not operate, host, provide hosting facilities to or assist in anyway 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.



## Internet Usage

Where a caching server is provided as part of the broadband managed service, schools must not relocate the caching server, change the admin password or modify its IP address without informing their LA and Northern Grid.

Attempts to access illegal sites banned by the Internet Watch Foundation will result in the user being automatically reported to the appropriate police authorities and may result in legal or civil actions.

Documents which are defamatory or intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability are not allowed and may result in disconnection, legal, disciplinary or civil action.

## Best Practice Guidance

checkbox

### Use of Passwords

It is strongly recommended that passwords are changed regularly and where the age of pupils allows, contain letters, characters and numbers.

### Email

School or work email addresses should not be used for personal use.

### Internet Filtering

Northern Grid for Learning's broadband network delivers Internet filtering which has national accreditation. Schools should not use any other filtering system without the express permission and approval of their Head Teacher and/or their LA. Information Risk Officers (IROs) should monitor Internet usage regularly and inappropriate use dealt with in line with the school's published AUP.

### Use of Mobile and Other Electronic Devices

It is strongly recommended that mobile devices access the Internet via the filtering provided by Northern Grid. Any mobile device must not negatively impact on the network and must be checked for viruses and spam content before being attached

### Social Media

Use of social media should carefully considered to ensure all members of the school community are kept safe. Schools need a social networking policy based on a risk assessment.

### Taking and Storing Images

Images that involve children should not identify children by name and permission should have been agreed by the subject and/or relevant parent / carer before posting. 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.

### Use of Video Conferencing

All users are advised to use the JCVS system for on demand or pre-booked VC session.

### Data Handling and Data Transfer

All data referring to individuals or that contains sensitive information should be encrypted.

## Reporting Accidental Access to Inappropriate Material

Any user who comes across inappropriate or offensive material should:

- Inform the website address to the school's eSafety or Information Risk officer
- Request a log of the web address, time and username in the incident log
- The school's eSafety officer should contact Northern Grid and/or their LA representative to initiate an investigation. The categorisation will be checked.
- If global blocking is not approved, the LA/ school should block the site locally.

## Reporting Suspected Deliberate Abuse or Misuse

Any person suspected of deliberate misuse or abuse should be:

- Reported to the school eSafety officer, IRO or Head Teacher
- The Head Teacher should inform the Local Authority.
- The Local Authority should complete an internal investigation form, requiring Northern Grid to complete an internal investigation.
- Northern Grid will report inappropriate behaviour to the relevant authority. This may be the Local Authority or the School's Board of Governors.
- Confirmation of access to illegal materials or the committing of illegal acts, will be reported to the relevant police authority for investigation.
- 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.

## Reporting Accidental Access to Illegal Material

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

- Report the incident to the Head Teacher or senior manager
- Do not show anyone the content or make public the URL
- Make sure a reference is made of the incident in a log-book
- Go to the IWF website at [www.iwf.org.uk](http://www.iwf.org.uk) and click the report button
- If reporting a URL do not use copy and paste, type the URL