



Northern Grid for Learning

Acceptable Use Policy 2009

**Black Text = Original AUP & 2006 AUP
Blue Text = 2009 additions to AUP**

E SAFEGUARDING

E SAFEGUARDING

E SAFEGUARDING

WWW.NORTHERNGRID.ORG/ESAFETY

Enforceable

Introduction

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. Your LA has agreed to abide by this AUP. This policy applies to all users of the Northern Grid broadband network whether in school or Local Authority offices. [This includes all users whoever they are, whatever technology used, whenever and wherever they are if connected to the network. This also includes users whether within a directly connected establishment or users connecting to the network remotely.](#)

General Requirements

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 and / or civil, disciplinary or legal action being taken upon individuals, groups of individuals or establishments.

Monitoring and Reporting

Internet usage from 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 including being reported to your LA. Where authorised by a LA, Northern Grid will proactively monitor, log, report and investigate Internet access for an entire site or nominated users. Reporting on aggregate usage is performed on a regular basis.

Acceptable Use

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 [or of any material which falls into the categories mentioned below](#) through the Service.

Prohibited Behaviour

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 is violent](#)
- 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 or effect.
- [is in breach of fraud or any criminal activity legislation](#)

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.

E SAFEGUARDING

E SAFEGUARDING

E SAFEGUARDING

WWW.NORTHERNGRID.ORG/ESAFETY

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. [Any violations of the system or network security will result in machines and organisations being disconnected from the service.](#) 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.

National Education Network

Where the NEN 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 NEN. Any breach of industry good practice (as represented by the standards of the [London Internet Exchange](#)), or of the Acceptable Use Policies of other networks, that is likely to damage the reputation of the NEN may be regarded as a breach of this Policy.

E SAFEGUARDING

E SAFEGUARDING

E SAFEGUARDING

WWW.NORTHERNGRID.ORG/ESAFETY

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.

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. An example of this would include creating an external wireless network to deliver broadband to another external site. [Users are not permitted to resell or connect any part of the regional network to 3rd parties without the express consent of 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.

Identification of Users

All users of the Northern Grid network, including remote users, are required to have individual user names and passwords which will allow identification as part of any investigation. Users should ensure that their user names and passwords are protected from misuse by others. Any user found to be deliberately attempting to bypass filtering and security systems and protocols for example; **accessing proxy anonymiser sites, will be reported to their LA and run a severe risk of disconnection from the network.**

Use of Video Conferencing

All VC endpoints must be registered with the Northern Grid Gatekeeper to make and receive video calls. Please go to the paragraph "Use of Video Conferencing" in the Guidance section of this AUP.

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.

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.

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.

E SAFEGUARDING

E SAFEGUARDING

E SAFEGUARDING

WWW.NORTHERNGRID.ORG/ESAFETY

Internet Usage

Northern Grid and Easynet provide filtering via filtering solutions which are Becta accredited and where purchased, an Equinet CachePilot. Where a CachePilot is provided as part of the broadband managed service, schools must not disconnect the CachePilot or move it to different part of the network or IP address without informing their LA and Northern Grid. All computers and mobile devices which are part of the school provision must be directed through the CachePilot.

All school CachePilots are monitored as part of the managed system for e-safety and support purposes and a monthly report is sent to your LA. This report identifies CachePilots that cannot be seen by Easynet. Any changes to the CachePilot IP address and/or Administrator password must be reported to the Easynet helpdesk on 0845 333 4568. Any schools suspected of bypassing the CachePilot will be reported to their LA. The regional broadband service complies with banned sites listed by the Internet Watch Foundation. Attempts to access these **illegal** banned sites **will** result in the user being reported to the appropriate **police** authorities **and may** result 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.

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 partner AUPs please go to: <http://www.uk.easynet.net/legal/acceptable.asp>
<http://www.esafeeducation.com/>



Guidance

Use of Passwords

It is strongly recommended that passwords are changed regularly and where the age of pupils allows, contain letters, characters and numbers. For help and ideas on how to make passwords applicable to young users or those with special educational needs please visit the E-safety part of the Northern Grid website.

Email

It is recommended that school or work email addresses are not used for personal use.

Internet Filtering

Northern Grid for Learning's broadband network delivers Internet filtering which is Becta accredited. This is in line with the Byron report (2008). Schools should not use any other filtering system without the express permission of their Headteacher and approval by their LA. The filtering delivered by Northern Grid, works in conjunction with an Equinet CachePilot. On delivery to schools CachePilot default settings are applied in line with regionally agreed policy. Schools are permitted to alter some CachePilot settings but should only do so if newly allowed websites have been checked by the school's e-safety officer. It is recommended that schools keep logs of changes to CachePilot settings recording the date, time, user and details of websites that have been unblocked.

It is strongly recommended that an approved member of staff monitors Internet usage via the CachePilot on a regular basis and that any suspected inappropriate use is dealt with in line with the school's published AUP.

Use of Mobile Devices whether Owned by Schools or Individuals

It is strongly recommended that mobile devices access the Internet via the filtering provided through the CachePilot as described above.

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.

Storage of Images

Any 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. 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

All users are advised to use the JCVS system for on demand or pre-booked VC session. The JCVS service provides quality assurance and additional services and hides your VC endpoint E164 number. A 17 digit E164 number is like a telephone number with the international dialing code prefix.

To improve system security, dynamic registration of endpoints, to the Northern Grid gatekeeper, ceased on April 13 2009. The vast majority of currently active endpoints will have had their system registration locked down so will continue to work as normal. Any endpoints that are not active may not be able to register with the gatekeeper; if this occurs you will need to complete a manual registration request form.

To request manual registration with the NG gatekeeper complete the registration form at the link detailed below ensuring all fields are accurately completed. The following registration process will take a maximum of 2 working days.

<http://web.videonations.com/cgi-script/csFormbuilder/forms/ngfl-videoconference-endpoint-registration.htm>

If a request is urgent contact: mark.vinnicombe@northerngrid.org.uk during work hours.

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

1. Always book the VC session via the national JCVS 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.

Data Handling and Data Transfer

Requirements are being developed for protecting data when transmitted across a broadband network or the Internet. Good practice dictates that all data which refers to individuals or contains sensitive information of any kind should be encrypted. Schools should consult their LA ICT departments for specific information relevant to their situation.

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. The school's E-Safety officer should contact their LA representative. The LA representative will contact Northern Grid to initiate an investigation. The categorisation will be checked.
4. The outcome of the investigation will be relayed back to the LA representative
5. If it is decided that the website is not sufficiently inappropriate for global blocking, the LA/school will need to make a localised decision to block the website via the school's own CachePilot or other proxy server.

For more information on reporting issues relating to web browsing, suspicious email and potential illegal content please see the resources at the back of this AUP

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 investigation 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.

[Violence](#)

[Racism](#)

[Illegal drug taking and promotion of illegal drugs](#)

[Criminal skills, proxy avoidance and software piracy.](#)

Access to Illegal Material

If this investigation results in confirmation of access or attempted access to illegal materials or the committing of illegal acts, Northern Grid or Easynet will inform the relevant police authority who 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.

[Accessing extreme pornography \(for further detail go to \[www.govconnect.gov.uk\]\(http://www.govconnect.gov.uk\)\)](#)

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.org.uk and click the report button
5. If reporting a URL do not use copy and paste, type the URL

[For more information please see the resource at the back of this AUP.](#)

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 a 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.

For support or guidance in sending Northern Grid a RIPA Notice please contact;
gerry.boynes@northerngrid.org.uk

For further information relating to RIPA please go to: <http://security.homeoffice.gov.uk/ripa/about-ripa/>

For digital copies of the resources contained in this booklet, general information, guidance and further resources regarding e-safety please go to: www.northerngrid.org/esafety

E SAFEGUARDING

E SAFEGUARDING

E SAFEGUARDING

WWW.NORTHERNGRID.ORG/ESAFETY

Committing an Illegal Act - Did You Know?

1

Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence

2

If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or personally investigate**

3

Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material

4

Showing anyone else illegal material that you have received **is an illegal act**

5

Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material

6

Printing a copy of the material to give to someone else **is an illegal act** and is classed as distributing illegal material

7

Within 4 simple steps you could easily break the law 4 times. Each is a serious offence

8

Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it

9

Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate **you are not.**

Never personally investigate. If you open illegal content accidentally, report it to the Headteacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening.** Once the email has been logged and reported to the IWF delete it from your inbox. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

What to do with Suspicious Web Browsing

You are browsing on the Internet and you accidentally find a website that has potentially illegal material e.g. Child abuse images, Incitement to violence, race hate or extreme pornography

Report this website to your Headteacher and/or E-Safety officer. A written log should be kept of the site and the fact that the details were passed onto the IWF

Report this site to the IWF
Go to www.iwf.org.uk
Click on the report button and follow the instructions and their advice.
The IWF is the only organisation licensed to investigate illegal content

You are browsing on the Internet and find a site that contains inappropriate content e.g. abusive or bullying content, adult sexual material etc.

Report this site to your Headteacher and/or E-Safety officer. A written log should be kept of the site. A decision needs to be taken whether to ban the site. Your technical support should alter your cache filtering

To escalate this investigation your school should contact your LA representative. They will contact Northern Grid who will initiate the investigation. The site will be looked at and could be globally banned.

You are browsing on the Internet and find a site that you feel is inappropriate for an educational site i.e. gaming or inappropriate language

Report this site to your Headteacher and/or E-Safety officer. A decision needs to be taken whether to ban the site. Your technical support should alter your cache filtering categories

Most sites that are against the ethos of the school but are not offensive will need to be blocked locally at school. These sites are sometimes allowed in other schools and are unlikely to be blocked globally

Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk
They are licensed to investigate **you are not.**

Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material

Never show or email a URL to anyone else if you suspect that it contains illegal material – you will be committing an illegal act
Never personally investigate

Never personally investigate. If you open illegal content accidentally report it to the Headteacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening.** Once the site has been logged and reported to the IWF delete it from your PC. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content please see their website for information and advice.**

What to do with Suspicious Email

You receive an email that has potentially illegal material e.g. child abuse images, incitement to violence, race hate or extreme pornography

Report this email to your Headteacher and/or E-Safety officer. A written log should be kept of the email and the fact that it was passed onto the IWF

Report this email to the IWF
Go to www.iwf.org.uk
Click on the report button and follow the instructions and their advice.
The IWF is the only organisation licensed to investigate illegal content

You receive an email that contains inappropriate content e.g. abusive or bullying content, adult sexual material etc. This email is from someone you know within the school environment

Report this email to your Headteacher and/or E-Safety officer. A written log should be kept of the email. An investigation within the school or LA should be undertaken.

To escalate this investigation your school should contact your LA representative. They will contact Northern Grid to investigate further. Any results from the investigation will be sent to your LA representative.

You receive an email that contains inappropriate content e.g. adult sexual material, bad language etc. and this email is not from someone you know but is from what seems to be a 'real' (i.e. not a spam) email address

Report this email to your Headteacher and/or E-Safety officer. A written log should be kept of the email and where it was sent for investigation

Contact your LA who will authorise Northern Grid to investigate. NG will trace the sender's ISP and advise on further action. (such as contacting the sender's school/organisation to raise a complaint)

You receive an email that contains inappropriate content e.g. adult sexual material This email is not from someone you know and appears to be a SPAM email.

Report this email to your Headteacher and/or E-Safety officer. A written log should be kept of the email and where it was sent for investigation

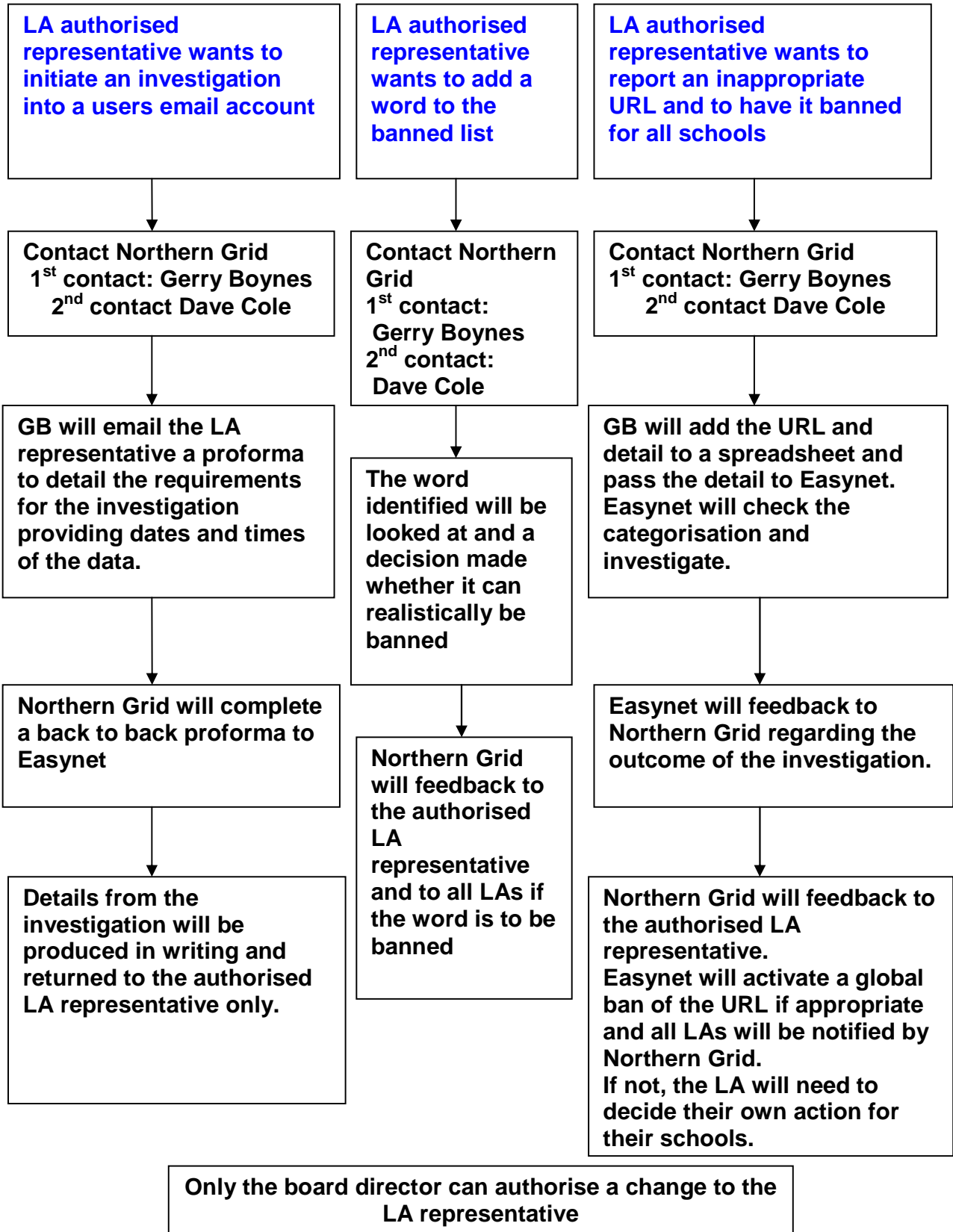
Report this to Easynet on abuse@uk.easynet.net
Or contact the Easynet helpdesk on: 0845 333 4568

In all cases secure the email in a folder and only delete when the investigation has been completed or you are advised to do so.

In the case of potential illegal material do not show the content of this email to anyone but report it to your Headteacher and take the advice of the Internet Watch Foundation.

Do NOT always presume that the sender's email address is telling you the truth – Spammers can and do fake other's email addresses. If you are unsure how to proceed please contact the Northern Grid for Learning on 0191 4611844

Process for E Safety Investigation



E SAFEGUARDING

E SAFEGUARDING

E SAFEGUARDING

WWW.NORTHERNGRID.ORG/ESAFETY