



How Safe is Your School?

The Internet is a wonderful resource providing information and learning activities. It has a darker side, of information not appropriate to learners. Schools should be aware of the potential dangers taking measures to ensure safe usage by all.

All schools have a responsibility to ensure that all pupils and staff access the internet safely and responsibly. Failure to do this could result in disciplinary or legal action taken against individuals, head teachers and governing bodies.

Schools culture and philosophy should determine the approach to online communications. Some schools have specific values and beliefs which should be reflected in their overall ICT policy use.

Every school needs an E-Safety committee. This should include senior school managers, governors, teacher, parent and pupils. The committee will set the standards and policy for the school's acceptable use of ICT.

All organisations need an Acceptable Use Policy. This sets out the rules and regulations for users. It identifies acceptable use and has clearly understood sanctions for any breach. Schools need to ensure that all staff and pupils understand the school's policy. It is recommended that all staff and pupils sign a contract to show that they have understood the policy and agree to its rules. Copies of sample Acceptable Use Policies can be found on the Northern Grid website: www.northerngrid.org.

Members of the SMT should be responsible for overseeing general security, administration and compliance with the agreed Acceptable Use Policy. Schools should monitor internet use by staff and pupils, policing the usage of their policy and imposing sanctions for misuse.

Northern Grid and Easynet provide internet services for schools within the partner authorities. This internet service fully meets the requirements of the Internet Watch Foundation. All illegal sites are automatically blocked and inaccessible by any user attached to the Northern Grid network.

Schools are responsible for ensuring that other inappropriate sites are blocked. These include pornography, gambling, race hate, drugs and weapons. Northern Grid provides schools with protection from these by installing an Equinet CachePilot at each school site. The CachePilot controls access to these sites and is managed by individual schools. Northern Grid strongly recommends that schools do not unblock these categories via the CachePilot. Administration rights should be strictly controlled.



Do the Following Quiz To Check the E-Safety of Your School

- Does my school have an E-Safety committee which agrees the general principles?
- Do we involve parents and pupils in identifying good practice and setting boundaries for use?
- Do we set clear sanctions for staff and pupil use?
- Do we monitor and police the policy and be strict about applying sanctions where necessary?

Acceptable Use Policies

- Do we have an acceptable use policy?
- Is it reviewed at least annually?
- Does everyone understand and follow it?
- Has it been signed by all staff and pupils to show compliance?

Use of the Internet:

- Do we know what kind of sites are allowed and not allowed?
- Does everyone know what they should do if they accidentally find a site which is offensive?

Use of email:

- Do you allow everyone to send emails outside of school?
- Does everyone understand the type of language which is acceptable in emails?
- Do you allow attachments to be sent and received?

Passwords:

- Does everyone have their own username and password which must be used to log on to the internet and email?
- Are passwords private?

- Are there sanctions for those who give their passwords to others or who misuse others' passwords?
- Are the administration passwords treated responsibly by those who have the right to use them?
- Do you know who has admin passwords in your school?

Viruses and Spam:

- Does your school have an up to date anti virus and anti spam system?
- Is it updated regularly?
- Is your network set up to automatically scan laptops, memory sticks and other portable devices when they are connected to your school network?

Cache Pilot Security

- Does your school use a CachePilot? If not, do you have a similar device which is as good?
- Is your CachePilot set up so that all computers access the Internet via the CachePilot?
- Do you know which sites have been blocked or allowed?
- Does the administration of the CachePilot reflect your E-Safety Committee's recommendations?

Video Conferencing

- Does your school's video conferencing system link to the regional and national VC networks?
- Do you use the national JVCS service to check that you are connecting to a bone fide site?

Mobile Devices

- Do you allow mobile devices to be used in school?
- Does your policy cover appropriate use of these?



Monitoring

- Does your school monitor and report on use of all your systems including the use of Internet and Email?
- Do all users understand that their use of the system may be monitored and reported on a regular basis?

General Network Security

- How do you know that your network is secure?
- If you use wireless, is this a secure encrypted service?

What to Do if Things Go Wrong

- Does your school have a clear system for dealing with emergencies?
- Do all users know what to do if they find emails or websites which are offensive?
- Do you have a system for logging action taken in the event of an emergency?

How Can the Northern Grid for Learning Help?

If the answers to these questions are “No” or “Don’t Know”, contact the Northern Grid or your Local Authority for help and advice.

Northern Grid for Learning staff have experience and knowledge in dealing with E-Safety issues. These include general design and content of AUPs, advice how to deal with systems in schools and technical help and support to ensure that all network systems are secure.

If you want more help and advice contact the Northern Grid team on:

admin@northerngrid.org.uk

or telephone 0191 4611844.