

Why is Internet access important?

The Internet is an essential element in 21st century life.. ICT skills and knowledge are vital to access life-long learning and employment, indeed ICT is now seen as a functional, essential life-skill along with English and Mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All children and young people should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to children and young people and the professional work of staff, for example:

- access to world-wide educational resources,
- access to experts in many fields,
- educational and cultural exchanges between children and young people worldwide,
- collaboration and communication within the wider context,
- access to learning wherever and whenever convenient.

The Internet enhances the management information and business administration systems for example within:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time 'remote' training support;
- secure data exchange between local and government bodies.

In support of this, the government provides a Standards Fund grant to support Local Authorities to procure broadband services through local Regional Broadband Consortia (RBC). In North Lincolnshire the Yorkshire and Humber Grid for Learning (YHGfL) is the RBC. North Lincolnshire schools and other establishments are connected onto this broadband network. The YHGfL is part of the National Education Network (NEN).

All English maintained schools are expected to be part of the NEN.

The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people. Much of the material on the Internet is published for an adult audience and some is unsuitable for Children and young people. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

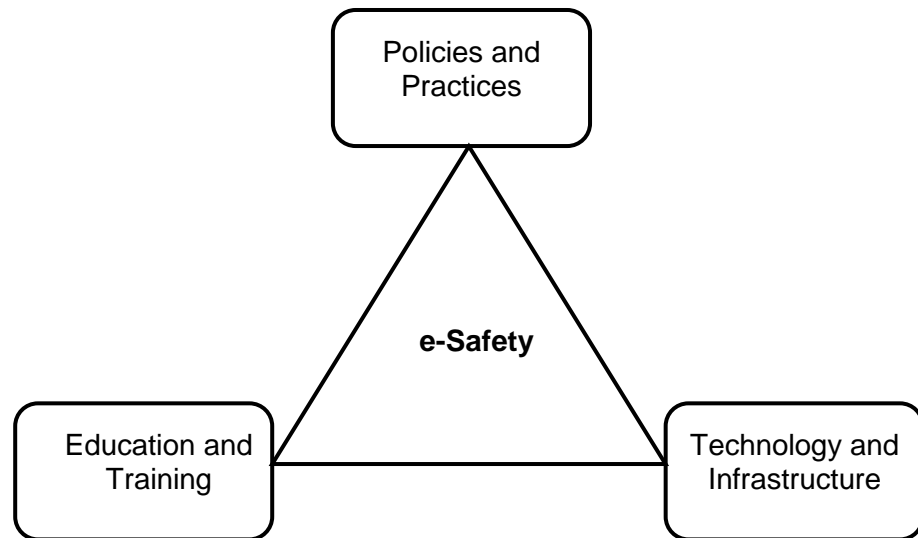
In line with policies that protect children and young people from other dangers, there is a requirement to provide as safe an Internet environment as possible and to teach children and young people to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture. The internet can pose risks and people working with children and young people should consider extending an education programme to parents and carers.

There are decency laws in relation to computer technology. It is a criminal offence to hold images of child abuse on computers or to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening emails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

Agencies working with children and young people need to make it clear that using equipment to view or transmit inappropriate material is “unauthorised” and infringements will be dealt with; and by ensuring that all reasonable and appropriate steps have been taken. Reasonable steps include technical and policy actions and an education programme for children, young people ,staff, and parents.

There are three core elements for an organization to address when considering e-safety:

Technology
Policy and Practices
Education and training



The following pages look at each in turn.

Technology and infrastructure: Background information

Internet filtering is a key service and all agencies need to ensure that they have adequate approved filtering systems in place. These should be routinely updated and monitored in partnership with their suppliers. Additionally, all individual systems should have up-to-date anti-virus, anti-spyware and anti-spamware software and approved firewall solutions installed on their network. YHGfL provide solutions for all of these and if used they should be set-up to be automatically updated so that networks remain up-to-date.

To make sure rogue applications are not downloaded and hackers cannot gain access to the equipment or into users' files, Children, young people and staff should not be able to download executable files and software. Unfortunately, inappropriate materials will inevitably get through any filtering system, therefore we should be vigilant and alert so that sites can be blocked. Conversely, if appropriate websites need to be unblocked you need to liaise with the headteacher. High level monitoring of website access is recommended that can lead to further investigations.

Filtering, coupled with child-friendly search engines [e.g. <http://yahooligans.yahoo.com/> | <http://www.askforkids.com/>] reduce the likelihood of children and young people finding inappropriate materials.

Caching some sites - so they are now essentially stored as off-line resources for viewing later from the Local Area Network (LAN) is another useful strategy. Our school has a cache server.

Children and young people can publish to the Internet through a safe, closed environment through the Regional Broadband Consortium.

Personal data should not be sent across the Internet unless it is encrypted or sent via secure systems.

Technical and Infrastructure

This Establishment

- Maintains filtered broadband connectivity.
- Works in partnership with the LA to ensure any concerns about the system are communicated. to the relevant officers so that systems remain robust and provide protection
- Has additional user-level filtering in-place.
- Ensures network health through appropriate anti-virus software and network set-up so staff, children and young people cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures their network is 'healthy' by annual health checks on the network
- Utilises caching as part of the network set-up;
- Ensures technical staff and Administrators are up-to-date with services and policies;
- Ensures that technical staff and Administrators check to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate.
- Never allows children or young people to access Internet logs;
- Uses 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Never send personal data over the Internet unless it is encrypted or otherwise secured;
- Never allow personal level data off-site unless it is on an encrypted device;
- Ensures children and young people only publish within appropriately secure learning environments such as their own closed secure YHGfL portal or Learning Platform.

Internet policy and procedures: background information

Due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. Whatever systems are in place, something could go wrong which places children and young people in an embarrassing or potentially dangerous situation. Awareness of the risks, having the appropriate systems in place and supervising children and young people are important considerations in reducing the risk

Surfing the Web

It is good practice to teach children and young people about appropriate internet use. Using favorites for a selection of websites is a useful strategy to focus children and young people on a task. Sites should always be previewed and checked, and work can often be best located on a closed Learning Platform.

Search Engines

Some common Internet search options are high risk, for example Google image search. Some LAs and Councils block this (at a corporate level). Others keep it unblocked because it can be a useful tool for children, young people and staff, however when used caution must be taken and ideally run in safe mode. [NB: Images usually have copyright attached to them.]

Collaborative Technologies

Collaborative technologies can be motivational, develop oracy and presentation skills and help children and young people consider content and audience. There are a number of collaborative technologies such as blogs, Wikis, video conferencing and RSS feeds that are effective communication tools that children and young people tap into. However, the use of social collaboration tools within a safe closed Learning Platform is recommended.

Social Networking Site

Social networking sites are environments that should be used with caution. Users need to know how to keep their personal information private, setting-up and using these environments safely. Children and young people need to be guided regarding safe behaviour whilst on these sites.

Chatrooms

Many sites allow for 'real-time' online chat. Again, children and young people should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Children and young people should be taught to understand the importance of safety within any chat room. For general advice and guidance for children, young people, parents/carers and staff please visit www.thinkuknow.co.uk

Sanctions and infringements

The establishments Internet e-safety / Acceptable Use policy is made available and explained to staff, children, young people and parents, with all signing acceptance / agreement forms appropriate to their age and role. The establishment needs to make clear the sanctions for infringements.

See associated Sanctions and infringement document.

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on a computer, the matter should be immediately referred to the Police. There are many instances where establishments, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.

Policy and procedures

This Establishment:

- Supervises children and young people's use at all times and is vigilant in the areas where young people have more flexible access;
- We use an appropriate and approved filtering system which blocks harmful and inappropriate sites;
- Websites to be used with children and young people should be previewed by staff.
- If raw image searches are used staff vigilance is crucial
- Informs users that Internet use is monitored;
- Informs children, young people and staff that they must report any failure of the filtering systems directly to the headteacher. Our systems administrators report to LA / YHGfL where necessary;
- Access to Chat rooms and social networking sites is not permitted. Only uses YHGfL for children and young people's own online creative areas such as web space and ePortfolio;
- Only uses the YHGfL / NEN service for video conferencing activity;
- Only uses approved or checked webcam sites;
- Has blocked children and young people's access to music download or shopping sites – except those approved for educational purposes.
- Requires children and young people, to individually sign an e-safety / acceptable use agreement form which is fully explained.
- For very young children the use of closed / simulated environments are used for education (eg email)
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse. Keeps a record, of any bullying or inappropriate behaviour for evidence in line with the school behaviour management policy;
- Ensures the named child protection officer has appropriate training in E safety;
- Ensures parents provide consent for their child to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement.
- Makes information on reporting offensive materials, abuse / bullying etc available for children, young people parents and carers and staff; inappropriate and/or offensive use of social networking sites by parents or pupils using off site computers will be subject to strict action including, if necessary, legal action.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training programme: background information

It is a sad fact that pupils will occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring. Children, young people and staff need to know how to respond responsibly if they come across material that they find distasteful, uncomfortable or threatening. For example: to turn off the monitor and report the incident to the responsible adult for inclusion in the list of blocked sites.

Children young people and staff must learn to recognise and avoid risks online and to become 'Internet Wise'. To STOP and THINK before they CLICK. Both need to understand how to ensure personal information is, and remains, private. Staff must not confuse or compromise their professional role with any personal online activity, for example inviting children and young people into their personal social networking site.

Children and young people also need to be 'savvy' about what they read, hear and see. In the same way that the quality of information received via radio, newspaper and television is variable, everyone needs to develop skills in selection and evaluation of Internet – based information. Just because something is published in text or on-line does not make it fact. It's therefore important that any education programme links to activities to help pupils evaluate what is fact, what is fiction and what is opinion, and that children and young people consider whether something is plausible or biased.

Information literacy skills therefore need to be taught. These include skills to 'read' content – (contextual clues including design, lay-out, text, use of images, links to and from the content), where the material originates from and how the content can be validated.

Often children and young people access reliable material but need to select that which is relevant to their needs,.. Children and young people should be taught research techniques including how to narrow down searches and how to skim and scan content.

The philosophy of sharing information across the Internet has increased the risk of children and young people infringing copyright and committing Plagiarism (the theft of ideas and works from another author and passing them off as one's own). For young people, there are numerous 'essay bank' websites offering access to essays for free or for a fee, often encouraging students to submit their own works. Young people should be aware of the issues around copyright and encouraged to look for copyright information on websites, so reinforcing their understanding of the importance this issue. They also need to be aware that plagiarism is not only cheating but where sufficient is copied, an illegal infringement of copyright also constitutes a criminal offence.

Children and young people also need to understand the dangers of using unfiltered web access at a location where parental controls or filtering have not been enabled. Children and young people should be encouraged never to chat through a website or over a webcam with people that they do not already know and trust in the real world and not to post details about themselves to a website, in a message or in a social networking environment.

Pupils and staff need to know how to deal with any Cyber Bullying incidents.

Children and young people need to know about the national agencies, such as Child Exploitation Online Protection (CEOP), <http://www.ceop.gov.uk/> – so that in an extreme case, they know how to "report abuse". Where they do communicate or publish work outside of the YHGFL environment or other approved educational environment, it should be under adult supervision wherever possible.

Children, young people and staff need to know appropriate netiquette in their general communications: So, to enable this, e-safety must be built into schemes of work as appropriate, to ensure children and young people are 'taught' safe behaviours and practice and that there is a 'No Blame' culture to enable children and young people to feel able to report any abuse, misuse or inappropriate content.

Key resources include:

- DfES/Becta
- [Internet Proficiency Scheme](#)
- [Signposts to Safety](#)
- [Childnet international](#)
- [Think U Know](#) .

Parents have an important role in supporting safe and effective use of the Internet by children and young people –There is a need to consider a rolling training programme of support. See parents’ resources on the web sites above.

Education and training

This Establishment:

- Fosters a ‘No Blame’ environment that encourages children and young people to tell a responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures children, young people and staff know what to do if they find inappropriate web material.
- Ensures children, young people and staff know what to do if there is a cyber-bullying incident;
- Ensures all children and young people know how to report abuse;
- Has a clear, progressive e-safety education programme built on LA / North Lincolnshire/ national guidance. Children and young people are taught a range of skills and behaviours appropriate to their age and experience, such as:
 - to STOP and THINK before they CLICK
 - to discriminate between fact, fiction and opinion;
 - to develop a range of strategies to validate and verify information before accepting its accuracy;
 - to skim and scan information;
 - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
 - to know some search engines / web sites that are more likely to bring effective results;
 - to know how to narrow down or refine a search;
 - to understand ‘Netiquette’ behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
 - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - to understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
 - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
 - to understand why they must not post pictures or videos of others without their permission;
 - children and young people to understand why and how some people will ‘groom’ young people for sexual reasons;
 - to know not to download any files – such as music files - without permission;
 - to have strategies for dealing with receipt of inappropriate materials;
- Ensures that when copying materials from the web, children, young people and staff understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that children young people and staff understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- Makes training available annually to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
 - Information leaflets

- demonstrations, practical sessions held at school;
- distribution of 'think u know' for parents materials
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

Autumn 2009

Reviewed Autumn 2010