E-Safety Policy

Written by: GB
Reviewed by: RS
Date of Last Review: May 2018

The Digital Age**:** where a wide range of different media content can be accessed through a wide range of devices in a wide range of places! And the technology continues to march on, and with it the range of content that is available. Your phone is no longer just a phone. It will take photographs, play music and probably connects to the internet. Your computer (or tablet) is not just for writing letters on or working out your finances, it is for playing games, watching films, listening to music and socialising with your 'friends'. The games console now provides fascinating, and sometimes frightening, realistic imagery of imaginary worlds in which you can become a part and mix, via the internet, with likeminded individuals. And this connectivity, the ability to link up with other people electronically is now wireless and, therefore, we are always 'on' wherever we are. Young people are probably more 'on' than their parents, carers and teachers. This is their world. They are often called digital natives, naturally assimilated into this connected digital world. This does not, however, mean that they naturally understand and have the wisdom to behave appropriately and safely in this connected digital world. It is up to us as adults in general, and parents, carers and teachers in particular, as digital immigrants, to understand their world as much as we can so that we can help and support them in developing their understanding and wisdom.

We recognise that within our schools and settings we can try to lock out the wider world and keep young people safe but it is important for us to teach them about the outside world, the world when they go home and log on in their bedroom, the world that is in their pocket via their phone and the world they experience on their games console. We need to ensure that we provide them with the resilience and tools to effectively cope with the 'inappropriate' material or contact that they may become exposed to at some point in their 'on line' lives. This is education for life. We need to teach our children so that they can know what to do and who to talk to keep themselves and others safe.

E-Safety: The Rationale

E-Safety encompasses the use of new technologies, internet and electronic communications such as Learning Platforms, mobile phones, Video Conferencing, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their on line experience.

.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from an approved Internet Service Provider using suitable filtering.
- National Education Network standards and specifications.

Oakfield Lodge School

- Our e-Safety Policy has been written by the school, building on the Cheshire e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: … Richard Stevens
- It was approved by the Governors on: May 18

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil and family use and will include filtering appropriate to the age of pupils.
- Pupils and families will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems and security will be reviewed regularly. *(Please refer to the Appendix 2)*
- Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.
- We have adopted Cheshire East County Council's security standards as laid out in (appendix 3)

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site or social media should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head of school will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected. *Please see Understanding Images, Appendix 4 for guidance on how to do this.*
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupils, parents, carers and social workers.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents may be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be taught how to keep information private on social network sites and the importance of this
- Staff are advised that they should consider the consequences and possible repercussions of any information that they make available online, for example on a social networking site. Particular care should be taken in the posting of photographs, videos and information related to the school, school life, staff and pupils. (See Staff Acceptable Use Policy)
- All information published by the school on social media will be published in closed groups with invited stakeholders as members. One exception to this is Twitter. Twitter will be used to inform the local community about events at school. Al information published on this social network will not contain any information about pupils and will follow the Data Protection Act 1998.

Managing filtering

- The school will work with the LA, DCFS and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator (Rachael Denham) who should be known to all members of the school community.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. *Please see appendix*

Managing video conferencing

- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will not use personal equipment or non school personal electronic accounts when contacting students. They will be issued with a school phone where contact with pupils is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the local authority can accept liability for the material accessed, or any consequences of Internet access.

- The school will regularly audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Radicalisation and extremism

We have a duty to safeguarding pupils/students from potentially harmful and inappropriate on line material and will ensure appropriate filters and monitoring, and this will mean frequent audit checks on online activity in the school. We aim to prevent access to terrorist material and sites when accessing the internet in the school.

Responsibilities of the school community

Senior leadership's responsibilities

- Ensure adequate technical support is in place to maintain a secure ICT system

- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the Governors
- Develop and promote an E-safety culture within the school community
- Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have E-safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to E-Safety

E-safety co-ordinators responsibilities

- Promote an awareness and commitment to E-safety throughout the school
- Be the first point of contact in school on all E-safety matters
- Create and maintain E-Safety policies and procedures
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum
- Ensure that E-Safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff , who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy
- Monitor and report on E-safety issues to the E-safety group, the Leadership team and Governors as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Ensure an E-safety incident log is kept up-to-date

Responsibilities of all staff

- Read, understand and help promote the school's E-safety policies and guidance

- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current E-safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Embed E-safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Record all E-safety incidents on the incident log and report them to the E-safety Co-ordinator (Rachael Denham) or The safeguarding lead (Gemma Bailey)

Responsibilities of pupils

- Read, understand and adhere to the pupil AUP
- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all E-safety incidents to appropriate members of staff
- Discuss E-safety issues with family and friends in an open and honest way

Responsibilities of parents and carers

- Help and support the school in promoting E-safety
- Read, understand and promote the pupil AUP with their children
- Discuss E-safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Responsibilities of governors

- Read, understand, contribute to and help promote the school's E-safety policies and guidance as part of the schools overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-safety awareness

Complaints

- Complaints of Internet misuse will be dealt with by the E-safety lead (Rachael Denham) or the safeguarding lead (Sarah Martin) or deputy safeguarding lead (Nick Richards)
- Any complaint about staff misuse must be referred to the head of school.
- Complaints of a child protection nature must be dealt with in accordance with safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Cyberbullying

The Department for Education define cyberbullying as when: one person, or a group of people, tries to threaten or embarrass someone else using a mobile phone or the internet.

We take Cyberbullying as seriously as any other form of bullying. Any incidents involving pupils will be addressed in accordance with our Anti bullying policy (available on the school website.)

Where cyberbullying is occurring outside of school but it effects the emotional wellbeing of a pupil, school will take the appropriate action.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be discussed with the pupils at the start of each year and they will be reminded of them on a regular basis.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy on the school Web site.
- All parents will be invited to E-safety workshops in school so they understand E-safety.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to; access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. The Learning Platform.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. File names should not refer to the pupil by name.
Communicating ideas within chat rooms or online forums.	Only chat rooms contained with the schools Learning Platform and linked to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.

Appendix 2

Considerations around access to data from, into and within the school are as follows

1. Where a school is part of the Connected Cheshire network then external security to and from the school is managed by firewalls administered by Connected Cheshire.
2. Additional protection is provided by filtering services for web traffic and external email traffic which are managed by Connected Cheshire. Where a school has a concern that filtering is not blocking inappropriate websites it is their responsibility to contact Connected Cheshire Help Desk to report the website. Secondary Schools can manage their filtering over and beyond the service provided by Connected Cheshire.
3. Where a school buys into a third party ISP service then generally the responsibility to provide firewalls and filtering services is with the schools.
4. Schools should take responsibility for deciding who is allowed access to data within and external to the school through the use of an authentication policy (user identification and passwords need to be issued and managed)
5. It is the school's responsibility to ensure that the security of any wireless networks is set to block unauthorised access. Where possible the school should seek to upgrade systems to meet the County recommended standard which is available from the ICT section on the Cheshire Learning Portal.
6. It is good practice to set screen savers to engage after a maximum of 20 minutes which **require the user to log back** in when deactivated. This helps maintain security of systems by minimising the risk of computers being left logged on for extended periods of time and enabling user accounts to be abused by unauthorised users.
7. Virus protection should be installed on every computer and should be set to update automatically at least every week if not daily.

Appendix 3
Extracted from **Electronic Information, Communication & Technology Security Policy**

Controlling Access to ICT Systems and Assets

This section covers protecting both physical and logical access to Cheshire East County Council ICT systems and assets and how those assets are classified. It does not cover general physical access to buildings and protection of non-ICT assets.

4.1 Asset Classification

Objective: In order to maintain appropriate protection of ICT assets it is necessary to control access to them based on a classification of their criticality to the business and the risk.

Policy: *All of the council's ICT assets must be identified, classified and have a nominated custodian.*

For the purposes of interpreting this policy, ICT assets may be any of the following:

Information assets databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, archived information etc.

Physical assets computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PABXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), offsite facilities.

Software assets application software, system software, development tools and utilities etc.

Services computing and communications services, e.g. Telecoms, Internet service providers, hosting services, etc.

Physical & Environmental Security

Objective: physical and environmental security is used to prevent unauthorised access, damage and interference with ICT systems and services.

Policy Statement: *All physical access or connection to critical ICT resources used to process, store, display or transmit council information shall be physically protected by suitable mechanisms or methods in order to minimise the risk of malicious damage, tampering or unauthorised access.*

Logical Access

Objective: to maintain the security of ICT resources by reducing the risk of unauthorised access and by enabling unauthorised access/activity to be quickly identified.

Policy: *All access or connection to IT resources used to process, store, display or transmit council information must be:*

- *Formally authorised*
- *Via an approved authentication process (i.e. positively recognised)*
- *Accountable to an individual*
- *Restricted to functionality and data appropriate to an individuals job function*
- *Administered in a controlled manner*
- *Monitored for potential unauthorised access*

Passwords

Objectives:

- To prevent unauthorised parties from obtaining access to council resources
- To ensure passwords are a secure and cost effective access control mechanism
- o ensure employees understand the requirements of the password policy.

Policy Statement: *users must use strong passwords that adhere to the password guidelines*

Network Security

Objective: To prevent unauthorised access to Cheshire East County Council's ICT assets and information via networked services and to ensure the confidentiality, integrity and availability of information.

Policy Statement: *Access to both internal and external networked services must be controlled in order to prevent or detect unauthorised external connections. Minimum access permissions will be granted to enable such connections to fulfil their purpose. All external connections must have the provision for being monitored.*

Remote Access Services

Objective: to prevent unauthorised access to Cheshire East County Council's ICT assets and information by remote access /dial up methods.

Policy Statement: *Remote access to business information across public networks using mobile computing facilities should only take place after successful identification and authentication, and with suitable access control mechanisms in place. These will include encryption and strong authentication in relation to the sensitivity and confidentiality of the information.*

Teleworking

Objective: to ensure suitable protection of the teleworking site against the theft of equipment and information, the unauthorised disclosure of information, unauthorised remote access to the organisation's internal systems or misuse of facilities**.**

Policy Statement: *Management must authorise and control teleworking and ensure that suitable security and controls are in place for this way of working and that these comply with the Cheshire East County Council's Security Policy*

1.4.3 Wireless Networks

Objective To ensure that only authorised individuals gain wireless access to the network and that wireless transmissions cannot be monitored.

Policy Statement: *Wireless access must be authorised, authenticated, encrypted and permitted only from approved locations*. *Any wireless access to the network must be 'agreed with the ICT Security Manager and the business owner*.

Use of Electronic Communications

5.1 General Policy

Objectives:

- To encourage the proper use of Cheshire East County Council's electronic communications.
- To document what is considered appropriate usage.
- To ensure that employees are aware and understand their responsibilities.
- To prevent the misuse of Cheshire East County Council's electronic communications resources
- To clarify to employees the circumstances under which they may use the County Council's communications and information systems for personal use
- To communicate the implications to staff of not complying with the policies

Policy Statement: *Electronic communications resources must only be used for conducting the business of and/or furthering the business interests of Cheshire East County Council unless otherwise authorised by a senior departmental manager.*

Note: the use of email or Internet access for personal use may differ in some departments. Consult your line manager or the ICT Strategy Policy & Security Manager if in any doubt. Further details of what constitutes acceptable use can be found in the authority's "Communications and Information acceptable use policy"**.**

This policy covers all forms of electronic communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use, for example:

- mail systems (internal and external)
- internet and intranet (email, web access and video conferencing)
- telephones (hard wired and mobile)
- pagers
- fax equipment
- computers/laptops/tablets
- photocopying, printing and reproduction equipment
- recording / playback equipment
- documents and publications (any type or format)

The policy applies to all employees, agency staff and to other people acting in a similar capacity to an employee. It also applies to staff or contractors and other individuals providing services / support to the Council (e.g. volunteers). A similar policy exists in relation to elected Members, adjusted to reflect their unique role in the Council. Further details can be obtained from the County Secretary.

5.2 Electronic Mail (Email)

Objective: To protect the ICT assets and reputation of Cheshire East County Council by communicating to Cheshire East County Council employees and third parties:

- the way in which electronic mail (email) should be used (acceptable use) in the organisation
- the usage of email that is considered unacceptable (misuse)
- the security implications of using email
- the implications of breaching the policies.

Policy Statement: *Email must only be used for legitimate business purposes in accordance with the*

Internet Security Policy

Objective: The objectives of this policy are to protect the ICT assets and reputation of Cheshire East County Council by communicating to Cheshire East County Council employees and third parties:

- the way in which the Internet should be used (acceptable use) in the organisation
- the usage of the Internet that is considered unacceptable (misuse)

- the security implications of using the Internet
- the implications of breaching the policies.

Policy Statement: *The Internet must be used in the same way as other business information tools and used for legitimate business purposes in accordance with the* "Communications and Information acceptable use policy*..*

User Equipment (Workstations, PCs and Terminals)

Equipment on Cheshire County Council Sites

Objective: To ensure all Cheshire East County Council users and contractors are aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

Policy Statement: *All PCs, terminals and workstations must be secured from unauthorised access when left unattended*.

Mobile computing

Objective: To ensure that mobile computing equipment is used in such a way as to ensure the protection of Cheshire East County Councils physical and information assets.

Appendix 4
Understanding Images

Purpose of Guide
This guide is designed to raise awareness of how digital images work and how they can be modified to work efficiently and more safely on school websites. This guidance is for all users of learning platforms and websites including pupils. It will also support the efficient use of images in word processed documents, desktop publishing and presentations.

Background
Digital images can be acquired from a number of different sources including digital cameras, scanners, art packages and the internet. They come in a number of different formats, determined by their file suffixes such as *.bmp or *.jpg.

The BMP format is a common format created by art parckages such as Windows paint. Files in this format are in a raw format and are generally quite large. They are good for printing but can not be used on the internet.

The JPG format is commonly used by digital cameras, is compatible with the internet and the vast majority of applications. This is a compressed format and when files are saved in this format they will lose some of their quality. How determinable this loss is will depend on what you are using the images for. In general it will probably not affect you. Most digital cameras use JPG as their default setting.

There are other image types for different uses such as GIF, PNG and the proprietary formats used by graphics packages such as Photo Shop and Gimp. Different applications are able to read and use different file formats. The internet uses very few, jpg, png and gif being the most common.

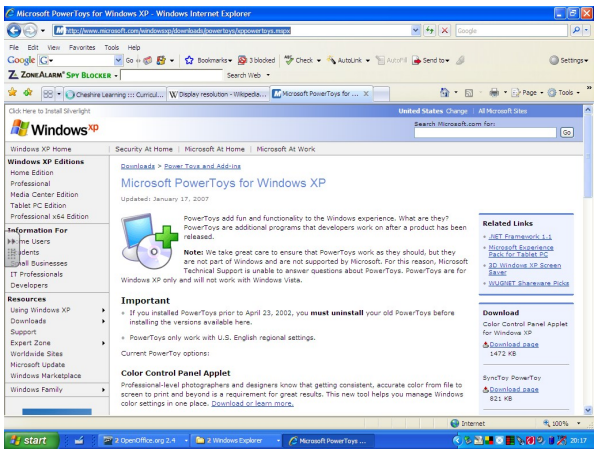
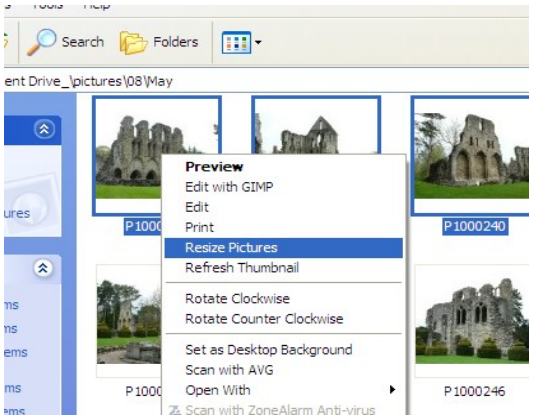
Computer screens use a variety of different resolutions and an understanding of these will help you determine the quality of the image you need to use. A typical set up in use today (May 2008) will use a resolution of 1280 X 1024 pixels. This is 1280 pixels wide by 1024 pixels deep. This is approximately the same resolution of a 1.3 mega pixel camera which means that this display would show the photograph at 100% of it's original size. Any better quality camera, i.e. a 5 mega pixel camera, would need the image reducing to show the full picture on the screen. Even the best quality monitors are only capable of displaying a 2 mega pixel image at full resolution. Many computer set-ups do not even reach the 1280 X 1024 resolution.

Modern cameras use very high resolutions to gain a better quality print but we do not gain the benefit of these resolutions on screen. In fact for most applications a large image is detrimental because it increases the time a document or file takes to load, whether it be from a local hard drive or over the internet.

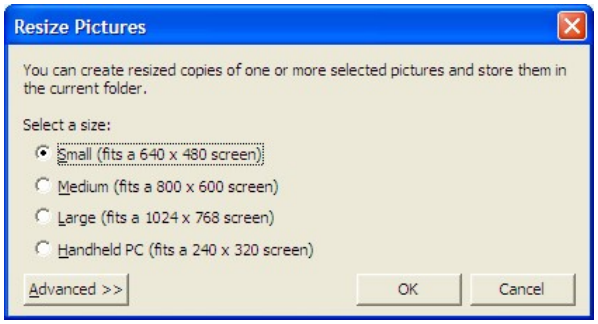
Perhaps the most concerning element is that images which are uploaded to the internet in their raw state, running to many mega pixels, can be easily downloaded and manipulated by the users of the website. This is easily done by right clicking on an image on the web and choosing Save Picture As.

The simple rule then is before uploading a digital image into a document or onto a website reduce it's size and resolution to the maximum needed to serve it's purpose. This will both help with performance and reduce the opportunity of images being manipulated.

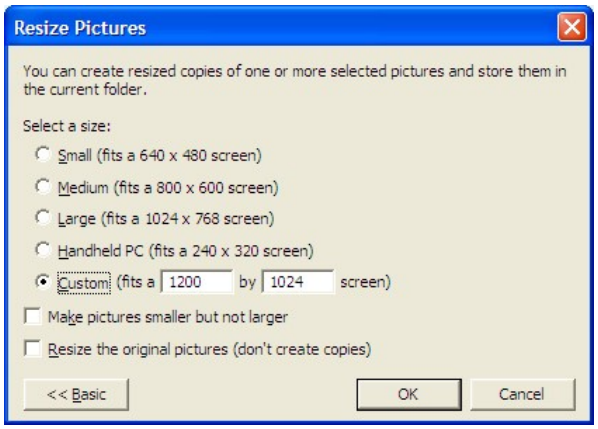
There are a number of ways to reduce the size of a digital image. The method suggested here is for use with Windows XP users and is the quickest and easiest way we have found, although there are others.

Download free of charge Image Resizer from Microsoft PowerToys at http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx. Install it on your system.	
Once installed find a folder with images in. You can highlight individual ones or multiple images. Once highlighted right click on them and select Resize Pictures from the menu bar.	

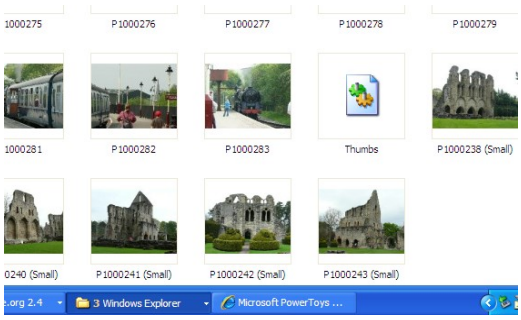
A menu comes up. All these will reduce the size of the file, and therefore the quality. A copy of the file will be created. You need to decide how big an image you need. Generally for a web page you are unlikely to need one that is bigger than the small one, and more likely you would need a smaller one still. You can tailor these in the advanced tab and selecting custom.



Unless you select the Resize the original pictures copies will be created in the same folder.



The pictures will be named with the same name and (small, medium, large or custom) in brackets. These images have been reduced in size from 3.7mb to 56k. This means that they will load much quicker on the web or keep the Powerpoint or word documents small in size. The user however will not see any noticeable difference in quality on the screen or even in an A4 print out of the document.



Recommendation

Teach all users and students how to manipulate images to reduce file size. Install software on all systems to make it simple to manipulate images.

Appendix 5
Guidance in response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any e-Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to e-safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Co-ordinator (Gemma Bailey), the e-Safety Officer (Rachael Denham) or the Police Liaison Officer.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

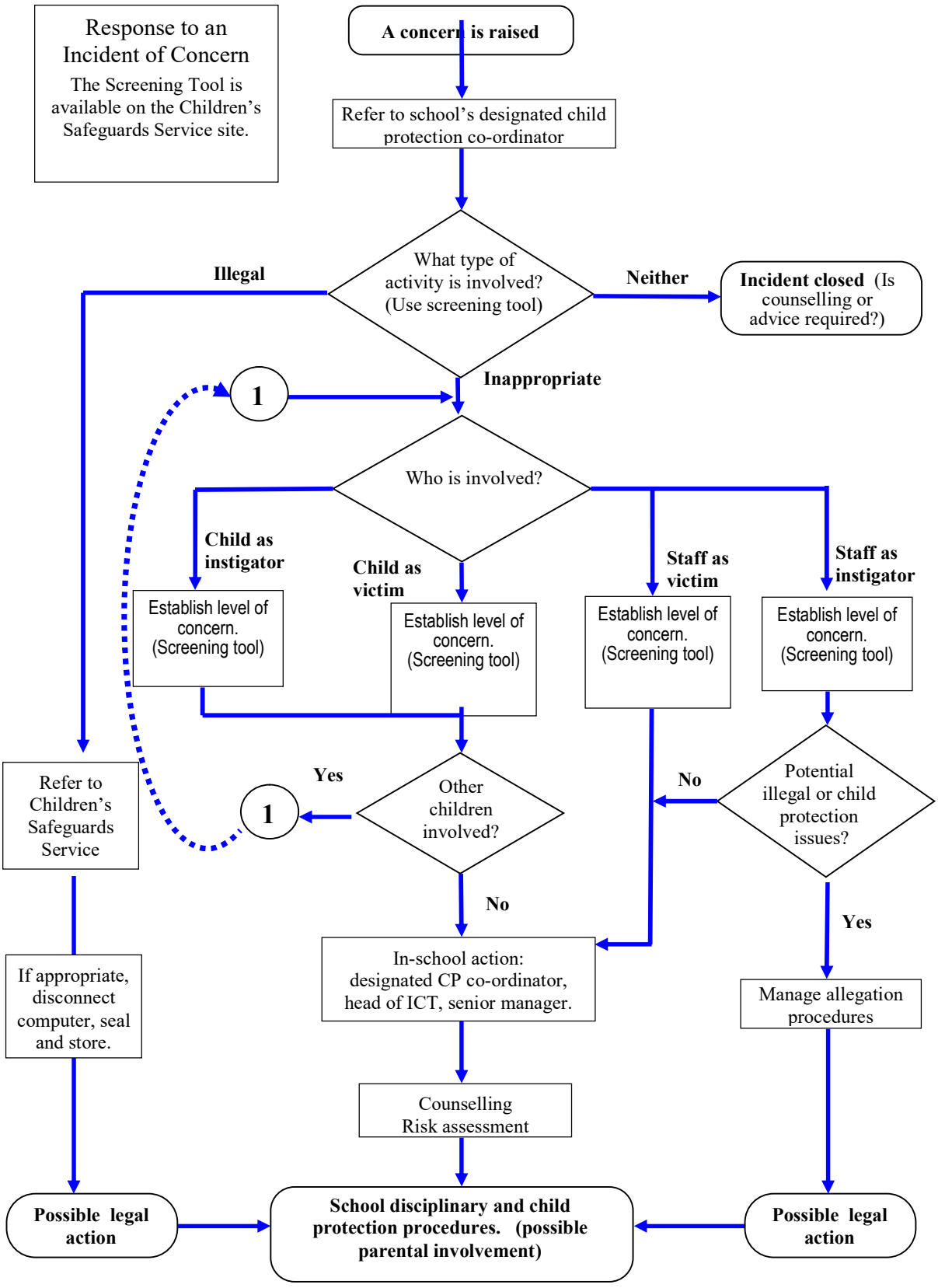
What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information / images
- Hacking and security breaches

How do we respond?

The flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Child Proctection Unit and Designated staff member should be consulted.

As previously stated schools should ensure that relevant policies (Acceptable Use Policy, Behaviour Policy, Bullying Policy, Discipline Policy) are referenced and are considered when dealing with the issues identified.


Response to an Incident of Concern
The Screening Tool is available on the Children's Safeguards Service site.
A concern is raised
Refer to school's designated child protection co-ordinator
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
1
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Refer to Children's Safeguards Service
Yes
Other children involved?
No
Potential illegal or child protection issues?
No
Yes
If appropriate, disconnect computer, seal and store.
In-school action: designated CP co-ordinator, head of ICT, senior manager.
Manage allegation procedures
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action

Appendix 6

Actions for inappropriate use

It is more likely that the school / academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Students / Pupils Incidents:	Refer to class teacher / tutor	Refer to Deputy Headteacher	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal		X	X	X		x			
Unauthorised use of non-educational sites during lessons	x						x	x	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x	x				x		x	
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x	x			x	x	x	
Unauthorised downloading or uploading of files	x	x			x	x	x	x	
Allowing others to access school / academy network	x	x			x				

by sharing username and passwords									
Attempting to access or accessing the school / academy network, using another student's / pupil's account	x	x				x	x		x
Attempting to access or accessing the school / academy network, using the account of a member of staff	x	x	x		x	x	x	x	x
Corrupting or destroying the data of other users	x	x	x		x	x	x	x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x			x	x	x	x
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x		x	x		x
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school		x	x						
Using proxy sites or other means to subvert the school's / academy's filtering system	x	x	x		x	x	x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident								x	
Deliberately accessing or trying to access offensive or pornographic material	x	x	x		x	x	x		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x		x	x	x		

Actions / Sanctions

Staff Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	x	x						
Unauthorised downloading or uploading of files	x	x						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x						
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x				x		
Deliberate actions to breach data protection or network security rules	x	x				x		x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x			x	x	x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x				x	x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	x	x				x	x	x
Actions which could compromise the staff member's professional standing	x	x				x		

Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	x	x				x		
Using proxy sites or other means to subvert the school's / academy's filtering system	x	x			x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x				x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x			x	x	x
Breaching copyright or licensing regulations	x	x	x			x	x	x
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x	x	x	x	x