THE CHURCH OF ENGLAND
Diocese of Chester

"In Our School There Is A World Of Wonder"

In our church school we are committed to ensuring that children feel safe, secure and happy in a climate of trust so that they learn to love themselves and understand and respect the views and needs of others.

We promise to provide a creative and nurturing environment in which children are encouraged to aspire to always do their best.

Woodcocks' Well CE VA PS

E-SAFETY POLICY

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: **V Booth**

What is E – Safety?

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, 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 online experience.

The school's e-safety policy will also run in conjunction with the Behaviour, anti-Bullying and Acceptable Use policies.

Rationale.

The Internet is now considered to be an essential part of modern life. In addition, the school has a duty to provide pupils with quality Internet access as part of their learning. This e-safety policy considers the use of both the fixed and mobile internet, PCs, laptops,

webcams, digital video equipment, mobile phones, camera phones, personal digital assistants and portable media players. It will be revised to incorporate new and emerging technologies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff, to improve communications between the school and parents and to enhance the school's management information systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use.

The school will ensure that all members of the school community are aware of the e-safety policy and the implications for the individual. E-safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies.

Guidance

End to End e-Safety

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 network including the effective management of Websense filtering.
- National Education Network standards and specifications.

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 day to day learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Where Internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils. All websites used for specific activities will have been approved by the school.

At Woodcocks' Well CE PS we use the internet for:

- Enriching teaching and learning through the curriculum
- As a shared teaching resource through use of educational sites such as Mathletics

- Accessing the school's website
- As a database of information to support learning
- To support the teaching of explicit ICT skills
- As a tool to support the teachers' planning and resource base

Internet use will enhance learning

- The school Internet access is designed primarily for pupil use and includes filtering appropriate to the age of pupils.
- Pupils and families (through e-safety workshops) 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
- The children access the internet to make use of Mathletics and other educational websites such as BBC Bitesize, whilst learning about safe and secure use of the internet, messaging, forums and personal web pages in a monitored and restricted access environment.

Managing Internet Access

Information system security

- School ICT systems and security will be reviewed regularly. *(Please refer to the Appendix 1)*
- 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's security standards as laid out in (appendix 2)

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published on the website.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The school Head Teacher and administrative staff will be responsible for communicating information and content to the person responsible for uploading and managing information on the school website, but this must be checked with the head teacher beforehand.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully; written permission will be obtained from children's parents or carers as to whether or not their photo can appear on the school website.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents on the website.

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 will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Staff will be 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 and they should refer the Staff Acceptable Use Policy.

- **Managing filtering**
- The school will work with the LA, DfE 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 ICT Coordinator who should be known to all members of the school community and then the issue should be referred to the LA ICT helpdesk.

Managing video conferencing -

In the event that video conferencing is used:

- 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 or parents. For further guidance, staff should refer to their Acceptable Use Policy.

Protecting personal data

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

Authorising Internet access

- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource.
- Within the Primary school access to the Internet will be supervised. Lower down the school staff will direct learning to specific, approved on-line materials.

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.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and in line with the school's complaint policy.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Introducing the e-safety policy to pupils

- E-safety rules will be displayed in each classroom.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be taught to follow the 10 rules for staying safe on-line as outlined below:
- *Don't give out personal info*
- *Tell if you find something that is not right*
- *Don't agree to meet people*

- *Never send your picture*
- *If some one says something mean online tell a grown up*
- *Don't do things online you know are wrong*
- *Check before you download anything*
- *Don't give out your password*
- *Set up rules for going on line*
- *Show your Parents and Carers how you use the internet. SHARE*

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff and governors with access to ICT equipment or learning platform will be asked to sign the Acceptable Use Policy

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety on the school Web site.
- Parents will be asked to talk to their children about the school's Acceptable Use Policy and staying safe on-line before signing and returning it to school

Date of Policy March 2016

Review Date March 2018

Signed…….Safeguarding Governor

Signed…….Head Teacher

Appendix 1

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 2

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

Correct of 12/10/08 Schools should keep up to date with this by accessing the CIS ICT Security Pages on the LA Intranet at
http://www.cccnet/services/CIS/CIS_R&D/ICT_Security/home.htm

4 Controlling Access to ICT Systems and Assets

This section covers protecting both physical and logical access to Cheshire 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.

4.2Physical & 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.*

4.3 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*

4.3.1 Passwords

Objectives:

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

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

4.4 Network Security

Objective: To prevent unauthorised access to Cheshire East'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.*

4.4.1 Remote Access Services

Objective: to prevent unauthorised access to Cheshire East'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.

1.4.2 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*.

5 Use of Electronic Communications

5.1 General Policy

Objectives:

- To encourage the proper use of Cheshire East'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'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 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
- 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 County Council by communicating to Cheshire 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* "Communications and Information acceptable use policy.

5.3 Internet Security Policy

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

5.4 User Equipment (Workstations, PCs and Terminals)

5.4.1 Equipment on Cheshire County Council Sites

Objective: To ensure all Cheshire 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.*

5.4.2 Mobile computing

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

Policy Statement: *Mobile computing devices, e.g. laptops, notebooks, PDAs and other handheld computing devices containing business information, must be protected to ensure information is not compromised or lost.*

5.5 Telephony Systems

Objective: To ensure that electronic communications using the telephone network are transacted between intended parties only, and are not subject to eavesdropping or interception.

Policy Statement: *Telephone networks must not be used for transmitting highly confidential or sensitive information where there is a risk that it can be overheard by others not authorised to receive it. If such a risk exists consideration should be given to alternative, more secure forms of transmitting the information including use of encrypted email (when available), postal communication or face to face contact.*

5.6 Software Policy

Objective: The software policy statement is intended to ensure Cheshire County Council meets all of its legal obligations regarding software licensing whilst protecting its ICT assets from security risks.

Policy Statement: *All software used on Cheshire County Council equipment or resources must be approved by the council, licensed and obtained by a council approved supplier. Cheshire County Council supports strict adherence to software vendors' license agreements. When at work, or when Cheshire County Council computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.*

5.7 Malicious Software Protection Policy

Objectives:

- To protect Cheshire County Council's ICT assets from damage, alteration or compromise from malicious software.

- To minimise the impact of a virus or malicious software once infection has occurred.

Policy Statement: *protection measures must be employed to protect Cheshire County Council's ICT assets from malicious software eg: viruses, spyware etc*:.

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.

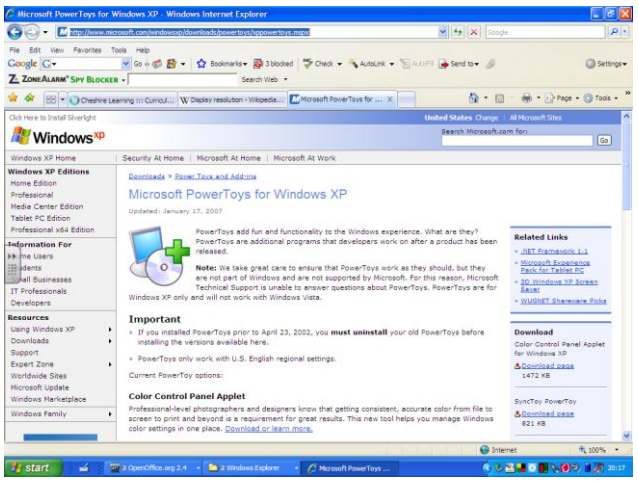
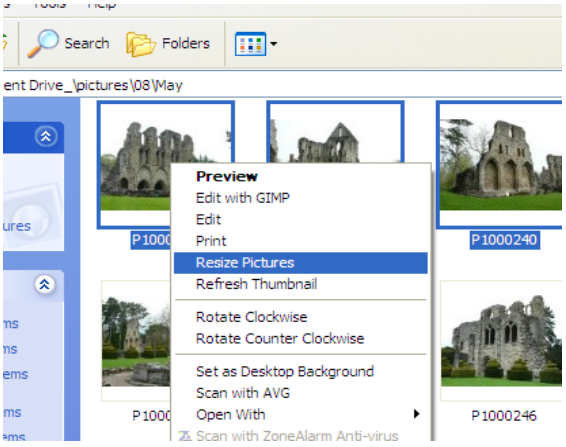
Modern cameras use very high resolutions to gain a better quality print but we do not gain the benefit of these resolutions on screen. In fact for most applications a large image is

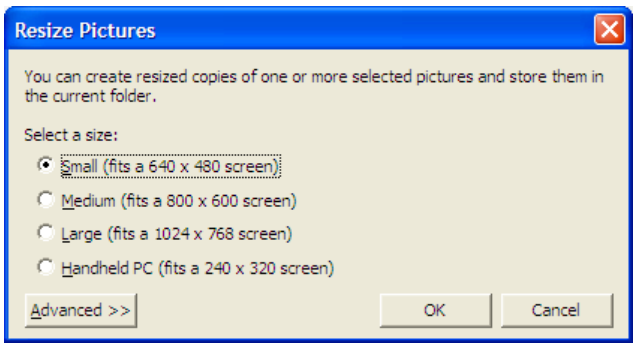
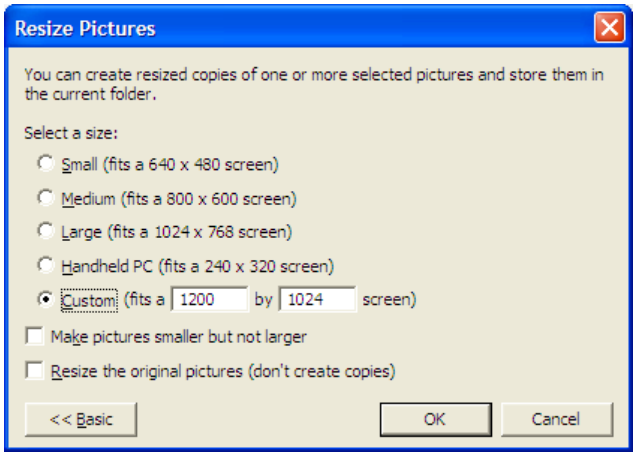
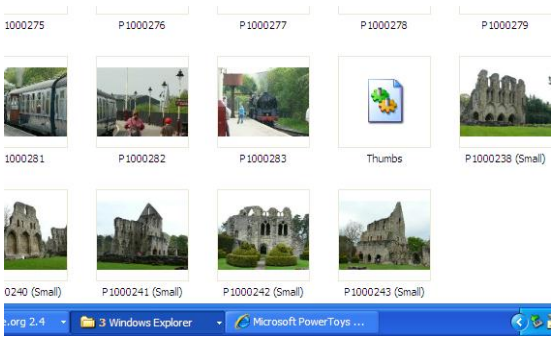
detrimental because it increases the time a document or file takes to load, whether it be from a local hard drive or over the internet.

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.

Guidance on 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. Photographs should not enable individual pupils to be identified. 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.

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, the e-Safety Officer 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**

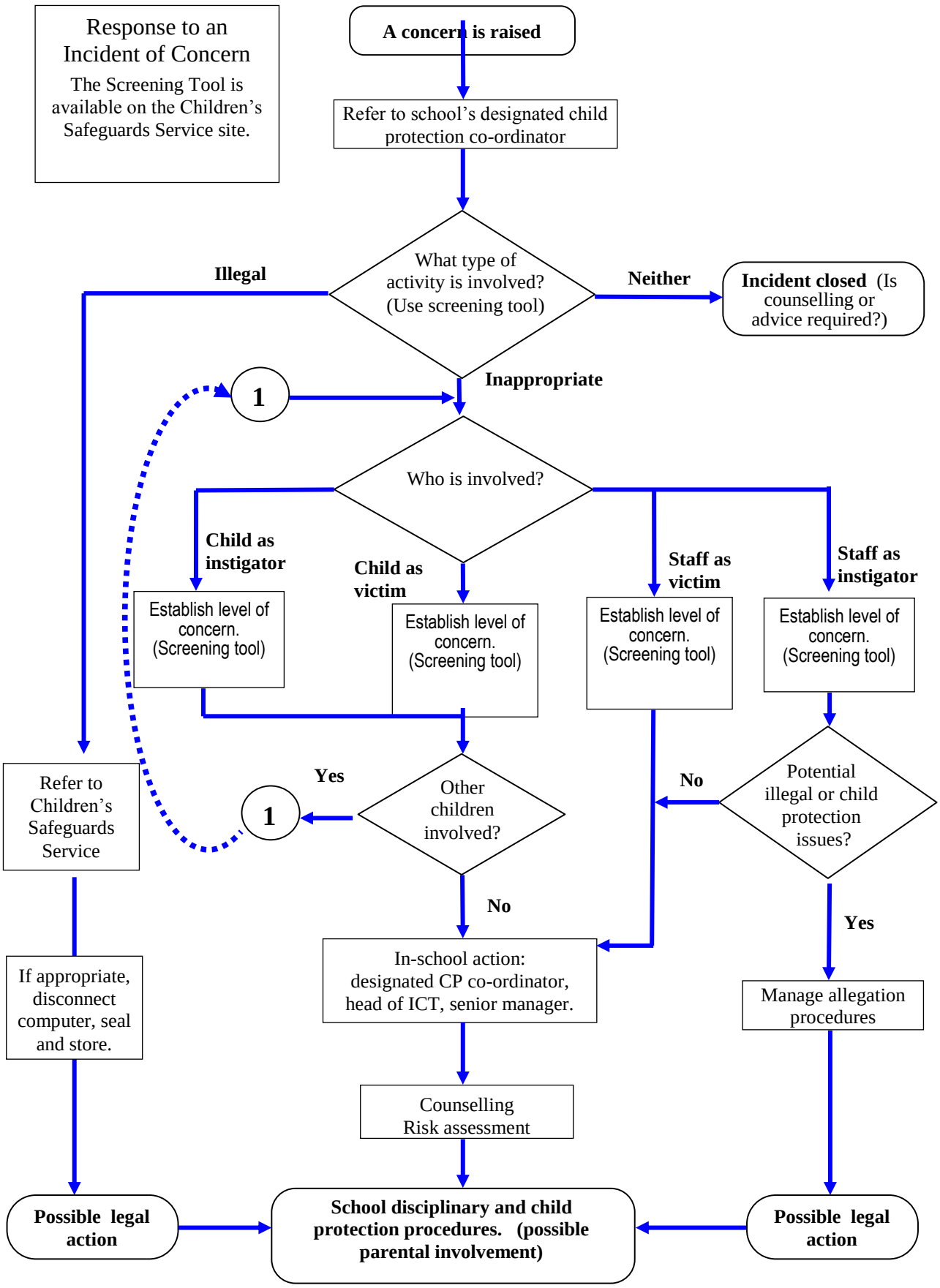
What are the risks?

- 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
1
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