Online Safety Policy

Werneth School Department of ICT

Internet Access and E-Safety Policy

Introduction

Werneth School will allow students, teachers and co professionals' access to the network services and the Internet. Using our and their own mobile electronic devices and computers.

All network activity and Internet access in school must be in support of education and or research and must be appropriate to the educational objective of the school. It is important that all network users are aware that systems are in place to track and record what is happening across the structured cabled network and wireless cloud. This policy applies to all members of the school community (including staff, students, volunteers' parents / carers, visitors andcommunity users) who have been granted a user account or access to the Werneth School ICT systems both in and out of school by remote connection.

Rationale

New technologies have become integral to the lives of children and young people in today's society both within schools and in their lives outside school. The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Correct use of electronic communication helps teachers and students to learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Werneth School has a duty to provide students with adequate Internet access to allow our digital natives to access resources to explore, enhance and develop their learning experience. Internet use is part of the statutory curriculum and a necessary tool for both staff and students. Correct use of online resources' is a necessary first order skill and one that we need to develop in our students so that they can become effective citizens and life long learners. The students and staff at Werneth School should have an entitlement to safe internet access at all times, however if misuse is an issue steps to restrict or prevent access will be put in place to safeguard the individuals and network infrastructure.

Roles and Responsibilities

The Headteacher is ultimately responsible for ensuring the safety of the students and staff at Werneth School (including e-safety). The Headteacher and the Senior Leadership team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff or student. It is important to

remember that most of the incidents of e-safety or online use issues are completely unique and have to be dealt with sensitively and depending on the incident it may include a number of key staff and possibility outside agencies

The headteacher at Werneth School has delegated the responsibility of e-safety security to a number of key staff within the ICT staffing structure. The director of ICT and e-services support team are responsible for Werneth Schools ICT infrastructure and it is their duty to ensure that it is secure and not open to misuse or malicious attack. All suspected misuse or problems must be reported to the e-safety coordinator and Headteacher. The school's Child Protection Officer and Child Protection Governor will be made aware of the potential for a serious child protection issue that could arise from the use of the Internet and other mobile handheld technologies connected to online resources.

Werneth School staff are aware that we all have a duty of care and should do our best to monitor the students activity when we provided electronic devices or computer access in our learning and teaching activities.

Curriculum

E-safety should be acknowledged in all areas of the curriculum and staff will reinforce e-safety messages in the use of ICT across the curriculum. In a developing school E-safety skills will be embedded and activities extended and developed through both discrete ICT and cross-curricular application.

In lessons where Internet use is pre—planned. It is best practice that students should be guided to sites checked as suitable for their use and that staff are able to quickly deal with any unsuitable material that is found in Internet searches. This can be done by a URL or Key Word blocking request or by using software classroom management tools such as RM Tutor.

Where students are allowed to freely search the internet, e.g. using search engines, staff will need to be vigilant in monitoring the content of the websites visited and use frequent review to keep the students on track and focused.

Throughout Key Stage 3 & 4 as staff we should in our teaching encourage students' to be critically aware of the materials and content they access on-line and should be guided to validate the accuracy of information to find. As teachers we need to embed the importance of acknowledging the sources of information, which they make use of and to respect copyright when using material accessed on the Internet. There is further guidance on this in the plagiarism policy guidelines document.

Responsible Internet Use and Safety

The school's responsible Internet use and e-safety policy shall govern all pupil access to the Internet. Parents will be informed that students will be provided with monitored and filtered Internet Access, Werneth School Zimbra Email and VLE accounts. As practicable as possible these accounts will be made accessible when a parent or carer has signed and returned the AUP and Internet use consent form.

Managing Filtering and Internet Security

Werneth School Internet access is designed for whole school use and includes filtering appropriate to the user group. (Staff, Administration and Pupil).

Internet use at Werneth School is filtered on two levels! First level filtering is provided at source by our Internet Service Provider Stockport LEA Business Services. The second level of filtering is provided on site by the e-services support team using a hardware firewall (Smoothwall). This second level of filter can be provided instantly.

Werneth School will take all reasonable precautions to ensure that users only access appropriate material. However due to the international scale and nature of the internet it is not possible to ensure that inappropriate material will never appear on a school computer. Neither the school nor Stockport Council can accept liability for the material accessed or any consequences of Internet access. To monitor student activity Werneth School has implemented a third layer of monitoring through a hardware device Securus. This system can be used to provide visual evidence of computer activity.

The school will work with the local authority. DFE and the Internet Service Provider to ensure that filtering systems are fully functional and live to protect students and we will regularly review the systems we have in place and improve them when necessary to provide safe, secure and robust access to online resources. If staff or students discover an unsuitable site it should be reported to a member of the E-services support team or E-Safety coordinator immediately.

The school ICT systems capacity and security will be regularly reviewed in conjunction with the school ICT director and the E-Services Support Team. Virus protection will be updated regularly and advice on security strategies from Stockport LEA will be discussed and implemented as necessary.

Safety

Students will be taught what is acceptable and what is not acceptable when using the Internet, and will be given clear objectives for Internet use. They will receive directly supervised access to specific approved on- line materials when ever practicable.

Students will be taught how to use the Internet safely when at school and encouraged to

follow these rules at home. Werneth School believes that e-safety issues should be embedded in all aspects of the curriculum and other school activities. Good practice will result in our students being frequently reminded of the rules for safe Internet and online use and the reasons for them. This is further enforced through the SECURUS monitoring system that enforces the students to a make and informed choice to accept the AUP every time they log on to the system.

ICT staff have planned a detailed and relevant E-Safety module, which is delivered to all years at key stage 3 and revisited at Key Stage 4 during Anti Bullying week and E Safety week. E-Safely advice will be provided as part of ICT, PHSE and parental engagement evenings this will cover both the use of ICT and new technologies in school and outside school. Werneth School values its partnership with parents and guardians and encourage them to set and convey the standards that students should follow when using the internet, and ensue that students understand and follow the school e-safety and acceptable use policy.

Werneth School believe that it is important that E-safety awareness is not limited to use of the Internet but also issues related to the use of mobile phones, cameras and handheld devices. Our school staff, students and parents have been provided with guidance and support on their use within lessons and in and around school. The Werneth School mobile devices policy is available for parents and staff on the Werneth School Website. Our school staff will monitor their use and implement current school policies with regard to these devices.

Werneth School will endeavor to make sure that staff and students are aware of the risks and legalities associated with the Internet which cover the following wide aspects:

- Exposure to inappropriate materials
- An awareness that the use of any internet and software materials must comply with copyright laws
- Inappropriate and illegaII behaviour
- Threats of physical danger

Students and staff will be made aware that actively seeking out; down loading or using information regarding these practices will result in disciplinary action.

Personal Security Guidelines

Werneth School will at all times encourage staff and students to adhere to the following guidelines;
Staff and Students should:

- Never reveal personal information - either their own or others, such as home addresses telephone numbers or personal email addresses.
- Never arrange to meet anyone they have contacted on the Internet without specific permission.
- Immediately notify a teacher, E-Service Team or Director of ICT if they come across information or messages that are dangerous, inappropriate or make them feel uncomfortable.
- Be aware that the author of one e-mail or web page may not be the person they claim to be.

Technical Infrastructure, Equipment, Filtering and Monitoring.

Werneth School will be responsible for ensuring that the school network is as safe and as secure as reasonably possible and that procedures approved within this policy are implemented. The headteacher and SLT team will ensure that the relevant people named in the above sections of this policy will be effective in carrying out their e-safety responsibilities. The school ICT systems will regularly be updated by the E-Services Support Team in consultation with the Director of ICT to ensure that key features of security such as anti virus definitions and Microsoft Windows Security updates are installed. It will be the sole responsibility of the E-Services support team to install only fully licensed software on the servers and client devices and ensure that Servers, wireless systems and structured cabling are securely located and physical access is restricted.

Passwords

All Staff and Students at Werneth School will be provided with a Username and Password for all active systems in order to access the network, Email and VLE. The Director of ICT and E-Services Support team will administrate access to the systems and access is tiered for functionality and security.

All users of the school learning platform will be provided with a username and password for secure access in school and remotely.

Use Of Chat Rooms

Students and staff will not be allowed access to chat roams, newsgroups, social networking sites or instant messaging services outside the Learning Platform.

Use Of Email

Staff and students may only use approved e-mail accounts on the school system. Users will be made aware that email communications on the school system may be monitored

by staff. Users must immediately report the receipt of any email that makes them feel uncomfortable, offensive, threatening or bullying in any nature and they must not respond to any such email. Any digital communication between staff and students or parents / carers will be professional in tone and content. As a safe guarding issue these communications should only take place on official school systems and personal email addresses, text messaging or public chat / social networking programs must not be used for these communications. With the increase use of Social Network sites such as Facebook and MySpace it is recommended to staff that they do not accept students as friend on their own personal accounts. Staff should have signed up to the staff AUP policy 2011.

Use of Handheld And Emerging Technologies

Use by students of portable media such as memory sticks, hand-held games consoles (e.g. PSPs), MP3 players (including IPods), and CD ROMs will be closely monitored as potential sources of computer viruses and inappropriate material. In an age where such devices are affordable to our students we as staff are to be vigilant in their use and monitor the students closely when these devices are being used.

Students should never use the school ICT network to download, load or install any software, shareware or freeware, or load any such software from disks etc on to clients. Mobile phones my be brought into school by students and they must be used within the mobile technology policy guidelines Staff and pupil mobile phones will not be used during lessons and the none use or granted signs should be displayed to communicate this to the students.

Use Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet to communicate or research information.

However, staff and students need to be aware of the risks associated with storing images and with posting digital images on the Internet. When using digital images staff should inform and educate students about the risks associated with the taking, using, storing, the publication and distribution of images.

School staff members are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: the personal equipment of staff should not be used for such purposes. Staff and students are to take great care when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Students must not share or distribute images of others without permission.

Photographs published on the school Learning Platform. Or elsewhere, that include students should be selected carefully and they must comply with good practice guidance on the use of such images. Childrens full names will not be used on the school web site in association with photographs.

Written permission from parents or carers must be obtained before photographs of students are published on the school Learning Platform.

Inappropriate Activities

Some Internet activity is illegal and is obviously banned from school ICT systems. There are however a range of activities which may, generally, be legal but would be inappropriate in school context either because of the age of the users or the nature of those activities staff should use their discretion and common sense.

Responding to Incidents Of Misuse

It is hoped that all members of our school community will be responsible users of ICT, who understand and follow this policy. However there may be times when infringements of the policy could take place, Through careless or irresponsible or very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Serious and Illegal Misuse

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct activity

then the response to an incident concern flow chart will be consulted and actions followed inline with the flow chart. In particular the sections on reporting the incident to the police and the preservation of evidence.

Inappropriate Misuse

It is more likely that the school 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 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.

Possible Pupil Sanctions.

If any pupil fails to follow the rules of conduct as described in the policy this could lead to sanctions being enforced, which may include:

- A temporary or permanent ban on the Internet or Network use within school.
- Additional disciplinary action in line with the schools behaviour policy.
- A ban on specific items being brought into the school (e.g. PSP, Mobile Phone).
- Parents and other agencies may be contacted.

Privacy

Teachers and the E-Service Support Team may review documents and log files to ensure that students and staff are using the system responsibly. If required Students and Staff will be made aware that their use of the Internet and network will be monitored. This monitoring takes place every time a member of the Werneth School Community accepts the SECURUS AUP.

Personal data held by the school will be recorded, processed transferred and made available according to the Data Protection Act 1988.

Staff Internet Access and E-safety

All staff, including teacher's classroom assistants and support staff will be provided with the responsible Internet use policy and its importance explained. Staff as well as students must accept the terms of responsible Internet use before using any school ICT resource. Staff will be made aware that.

Internet use may be monitored and traced and that could be by a senior manager and included the e-safety coordinator.

Staff must use their professional discretion to ensure that the school network, e-mail and Internet are at all times used in a professional manner. Werneth School expects staff to act as good role models in their use of ICT, the Internet and mobile devices

Staff Must Be Aware That

Any information downloaded must be respectful of copyright property rights and privacy.

Information is stored in the system and may therefore be observed by third party, including students.

Downloading explicit or offensive material, unlicensed software or software for personal use, may result in disciplinary response by the school or authorities.

Any information stored on computers must be mindful of confidentiality, data security and not conflict with school or Stockport council policies.

Any offensive or inappropriate sites, which escape a block by filtering, must be reported immediately to the E-safety coordinator or E-Services Team.

If illegal behaviour by a staff member is suspected, the school has a duty to consult with the police at the earliest opportunity, preserving any potential evidence.

Staff Laptop Use

A laptop issued to a member of staff remains the property of Werneth School. Users of such equipment must therefore adhere to the school policy regarding appropriate use with regard to Internet access, data protection and use of software. Users of laptops must be aware that inappropriate use of the Internet outside of school while using a school laptop will constitute a breech of the policy and result in disciplinary action. Staff will be made aware that the school must have a license before any software is loaded onto the computer and that no software should be loaded without permission from the ICT coordinator or E-Services Support Team. Staff also need to be made aware that storing photos of children on laptops may be considered as storing personal and sensitive information about a pupil. Staff will therefore be advised not to store photos on laptops due to their sensitive nature and the opportunities for misuse outside of Werneth School by anyone with access to the laptop. This will also apply to the storing of photos, or possibly sensitive information, on camera phones. Memory sticks and digital cameras by staff. All devices that are removed from the school site need to be encrypted so that data cannot be accessed easily. For further guidance see the Encryption Policy.

School Learning Platform and Website

The school learning platform aims to be a useful tool for staff, parents and students, It contains information about the school and examples of children's work, The school web site will only display the official school contact details and the school address, email telephone and fax numbers. Staff and pupil's personal information will not be published on any of these devices. For information and to report any problems with the Werneth School Website please consult Miss S Mansfield

Photographs

Photographs including students add interest to a school learning platform and website, but the security of staff and students must come first. Students and Staff will not be named in photographs. Written permission from parents or carers will be obtained before photographs of students are published on the school website.

Children's Work

Examples of students work on the school website may include the first name of the child

who produced the work in order to provide them with recognition of their efforts.

Parental Support

Internet use in student's homes is increasing rapidly, as is the use of the Internet on associated hand held devices e.g. mobile phones. We know that at Werneth School students have unfiltered and unsupervised access to the Internet at home and on our school ground via their mobile devices. All parents and staff should be aware of the concerns and benefits of Internet use and should reinforce rules for safe Internet use regularly. The school encourages parents to discuss Internet safety with their children, and to be aware of how they are using both the Internet and associated portable devices, which may have access to online resources'.

Please Refer To The Following Legislation for Additional Information:

- **Computer misuse act 1990 Regardless of an individual's motivation, the Act makes it a criminal offence to gain:**
  1. access to computer files or software without permission (for example using another persons password to access files)
  2. unauthorised access, as above, in order to commit a further criminal act (such as fraud)
  3. impair the operation of a computer or program

  UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

- **The Data Protection Act 1998**
  The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
  http://www.hmso.gov.uk/acts/acts1998/19980029.htm

- **The Freedom of Information 2000**
- **Malicious Communications Act 1988**
  This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

- **Protection of Children Act 1978**

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

- **Regulation of Investigatory Powers Act 2000.**
  Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
  http://www.hmso.gov.uk/acts/acts2000/20000023.htm
- **Trade Marks 1994**
- **Copyright, Designs and Patents Act 1988**
  Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

- **Telecommunications Act 1984**
  The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
  http://www.hmso.gov.uk/si/si2000/20002699.htm

- **Criminal Justice and Pubic Order Act 1994**
  This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the

Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

- **Racial and Religious Hatred Act 2006**
  It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

- **Protection from Harassment Act 1997**
  A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

- **Sex Offences Act 2003**
  The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

- **Communications Act 2003 (section 127)**

  Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

- **Public Order Act 1986**
  This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

- **Obscene Publications Act 1959 aid 1964**
  Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

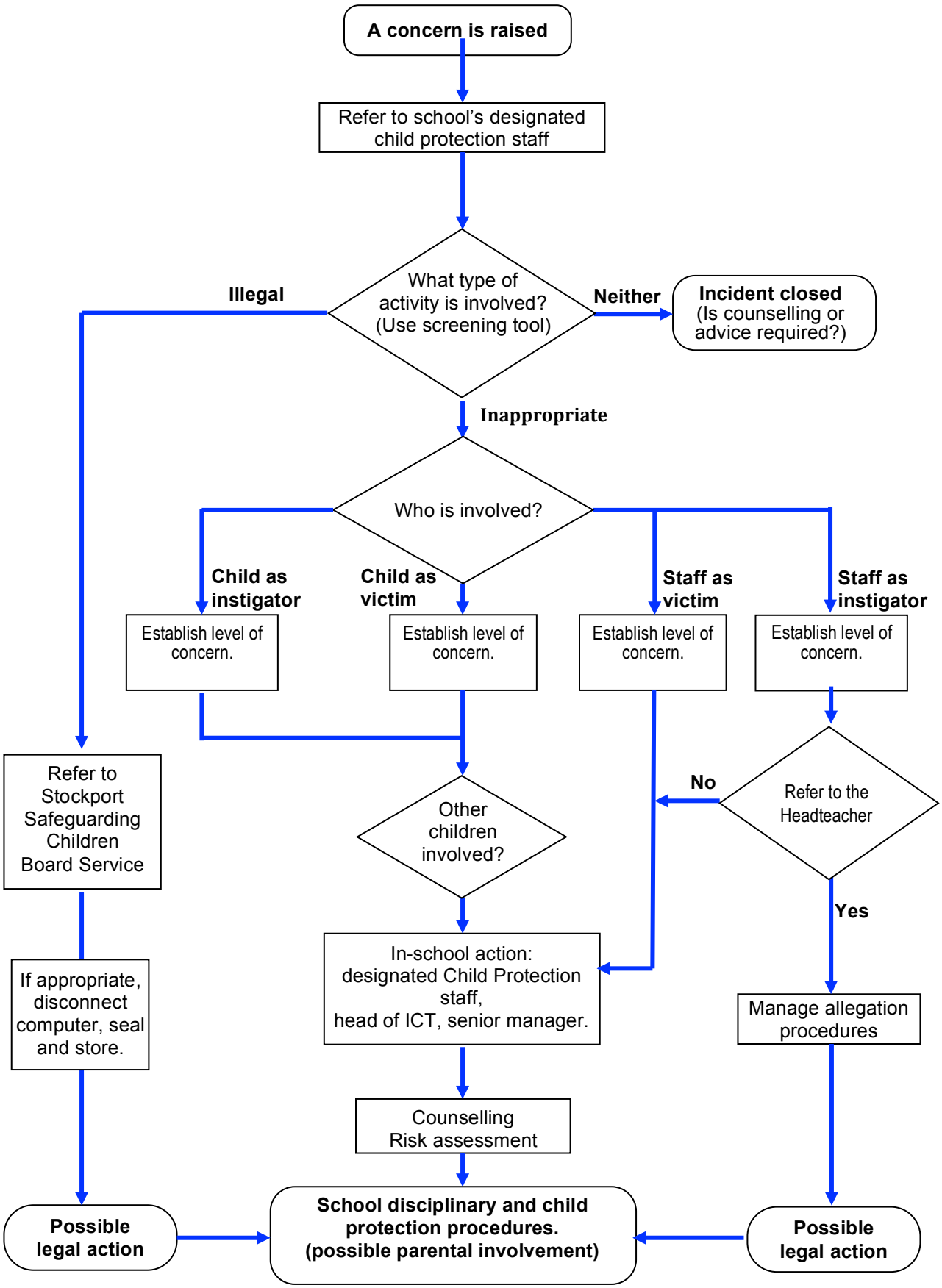
- **Human Rights Act 1998**
  http://www.hmso.gov.uk/acts/acts1998/19980042.htm

- **The Education and Inspections Act 2006**

Policy	Date modified	Date of approval	Review date	Governor Committee	Responsibility
Online Safety	January 2015	January 2015	January 2018	Resources	SBO

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images				✓	✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation				✓	✓
	adult material that potentially breaches the Obscene Publications Act in the UK				✓	✓
	criminally racist material in UK				✓	✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SMBC and/or the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet				✓	
Online gaming (educational)		✓			
Online gaming (non educational)				✓	
Online gambling				✓	
Online shopping/commerce			✓		
File sharing within school infrastructure based on professional duties			✓		
Use of social networking sites			✓		
Use of video broadcasting eg YouTube			✓		


A concern is raised
Refer to school's designated child protection staff
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern.
Establish level of concern.
Establish level of concern.
Establish level of concern.
Refer to Stockport Safeguarding Children Board Service
Other children involved?
No
Refer to the Headteacher
Yes
In-school action: designated Child Protection staff, head of ICT, senior manager.
If appropriate, disconnect computer, seal and store.
Manage allegation procedures
Counselling Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action