Policy for E-Safety

As agreed by the Governing Body – September 2015

To be reviewed – Annually

Contents

- School Personal Data Policy template
- School E-Safety Charter
- Ideas for schools to consider
- Legislation
- Links to other organisations and documents
- Resources
- Glossary of Terms

Background

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. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people will have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in our school are bound. The school's e-safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement

- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world. Therefore, this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. We therefore realise the necessity, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Churchfield C.E. (C) Primary will demonstrate that it has provided the necessary safeguards to help to manage and reduce these risks. This e-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Schedule for Development, Monitoring and Review

This e-safety policy was approved by the *Governor's Curriculum Sub Committee on:*	December 2013
The implementation of this e-safety policy will be monitored by the:	Senior Leadership Team (SLT) H.T., D.H. and Phase Leaders I.C.T. co-ordinator (curriculum)
Monitoring will take place at regular intervals:	Annually – end Autumn term
The *Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the SLT (which will include anonymous details of e-safety incidents) at regular intervals:	Once a year Compiled by Headteacher
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	December 2014
Will serious e-safety incidents take place, the following external persons / agencies will be informed:	LA I.C.T. Manager, LA Safeguarding Officer, Police Commissioner's Office LADO First Response

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Logs of monitoring of violations (Securus software)
- Feedback from pupils and staff

Scope of the Policy

This policy applies to all members of the school community (including pupils, staff, volunteers, parents/carers, visitors, Governors) who have access to and are users of school I.C.T. systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the E-Safety Policy. The Governors will receive regular information about e-safety incidents and monitoring reports. This will enable them to review the effectiveness of the policy.

A member of the Governing Body has taken the role of *E-Safety Governor.* Their role includes:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher ensures that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as appropriate
- The Headteacher ensures that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Phase Leaders are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- Phase Leaders receive regular monitoring reports from the E-Safety Co-ordinator through Leadership Team meetings.

E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place (shared role with I.C.T. Co-ordinator)
- provides training and advice for staff (shared role with I.C.T. Co-ordinator)
- liaises with the Local Authority
- liaises with school I.C.T. technical staff through I.C.T. Co-ordinator
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of Governors
- reports regularly to Leadership Team
- Meets regularly with I.C.T. Co-ordinator to discuss and ensure that e-safety aspects of the curriculum are fully covered

Network Manager (I.C.T. Co-ordinator) and Technical support staff:

Ensure:

- that the school's I.C.T. infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Staffordshire Learning Network provides the school with the RM solution 'Safety Net Plus'. The software is categorised into nine sections i.e. pornography, SMS messaging etc, by default several sections and websites are filtered and access is denied. The School is able to control their own permissions and add/amend to the defaults.
- the school's filtering policy is applied and updated on a regular basis
- that they are up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the school network, Virtual Learning Environment (VLE) and e-mail is regularly monitored in order to identify any misuse or attempted misuse. Violations detected will be reported to the E-Safety Co-ordinator for investigation, action and sanction as appropriate
- that monitoring software and systems are implemented on all curriculum computers (both pupil and staff) and that these are updated regularly (Securus software)

Teaching and Support Staff:

Ensure that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation, action and sanction as appropriate
- digital communications with pupils (e-mail / Virtual Learning Environment (Learning Platform)) will be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in any lesson where Internet use is pre-planned, pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches

Designated Person for Child Protection:

The Designated Person for Child Protection and Deputy Designated are trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

CPD will ensure that these roles remain aware of changes and potential risks.

Pupils:

- are responsible for using the school I.C.T. systems in accordance with the Pupil Acceptable Use Policy (AUP), which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They will also know and understand school policies on the use of images and on cyber-bullying.
- will understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of I.C.T. than their children. The school will therefore take every opportunity to help parents understand these issues by providing support in a variety of ways (*e.g. parents' information evenings, parent consultations, informative letters, website information, etc*).

Parents and carers are responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of I.C.T., P.S.H.E. or other lessons and will be regularly revisited – this will cover both the use of I.C.T. and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of I.C.T., the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of I.C.T. systems / internet will be posted in all rooms and displayed on log-on screens
- Staff will act as good role models in their use of I.C.T., the internet and mobile devices

Education – parents / carers

Parents and carers may have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents' information evenings

Education & Training – Staff
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- The E-Safety Coordinator will receive regular updates through attendance at ICT update meetings (QLS), training sessions and by reviewing guidance documents released by BECTA, Staffs LA / Entrust and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required.
- E-Safety Policy will be available to all staff through VLE (Learning Platform).

Training – Governors
Governors will take part in e-safety training and awareness sessions, with particular importance for those who are members of the curriculum sub-committee. This will be offered in a number of ways:

- Attendance at training provided by the Entrust, National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring
The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School I.C.T. systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school I.C.T. systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school I.C.T. systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed annually Governors.
- All users will be provided with a username and password by (system administrator) who will keep an up to date record of users and their usernames. Adult users will be required to change their passwords termly.
- The "administrator" passwords for the school I.C.T. system, used by the Network Manager will also be available to the Headteacher and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password, and they will not allow other users to access the systems using their log on details. Any suspicion or evidence that there has been a breach of security will be reported immediately to the Network Manager (I.C.T. Co-ordinator).
- The school maintains and supports the managed filtering service provided by the LA.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues will be reported immediately to Entrust.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Co-ordinator
- School I.C.T. technical staff regularly monitor (monthly) and record the activity of users on the school ICT systems using Securus software. Users are made aware of this in the Acceptable Use Policy and through visual prompts on all monitored computers
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system by issuing temporary accounts.
- An agreed policy is in place regarding the downloading of executable files by users – permission will be sought from Network Manager
- An agreed policy is in place regarding the extent of personal use that users (staff) and their family members are allowed on staff laptops and other

portable devices that may be used out of school. Refer to 'School Personal Data Policy' for further details.

- An agreed policy is in place that allows staff to install programmes on school workstations / portable devices. Prior permission is to be sought from the Network Manager.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices. Refer to 'School Personal Data Policy' for further detail
- The school infrastructure and individual workstations are protected by up to date virus software.

Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Refer to 'School Personal Data Policy' for further detail. Secure pen drives are provided for all staff.

Curriculum

E-safety will be a focus in all areas of the curriculum and staff will reinforce e-safety messages in the use of I.C.T. across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need.
- Pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet.

Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff 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 will only be taken on school equipment; the personal equipment of staff will not be used for such purposes.
- Care will be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website 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 website (through parental/carer acceptance of the AUP which is signed at the start of each academic year)
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software

the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones or other camera devices		✓ (with HT consent)						✓
Use of hand held devices eg PDAs, PSPs				✓				✓
Use of personal e-mail addresses in school, or on school network				✓				✓
Use of school e-mail for personal e-mails		✓			✓*			
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs	✓*				✓*			

** within the Learning Platform secure community environment*

When using communication technologies the school considers the following as good practice:

- The official school e-mail service may be regarded as safe and secure and is monitored. Staff and pupils will therefore use only the school e-mail service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users will be aware that e-mail communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.
- Any digital communication between staff and pupils or parents / carers (e-mail, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group e-mail addresses will be used in Foundation Stage, while pupils at K.S.1 and above will be provided with individual school e-mail addresses for educational use.
- Pupils will be taught about e-mail safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate e-mails and be reminded of the need to write e-mails clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the school website and only official e-mail addresses will be used to identify members of staff.

Unsuitable / inappropriate / illegal activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, will not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

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 SWGfL 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 (e.g. 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				✓	
On-line gaming (educational)	✓				
On-line gaming (non educational)				✓	
On-line gambling				✓	
On-line shopping / commerce				✓	
File sharing	✓				
Use of social networking sites				✓	
Use of video broadcasting eg Youtube			✓		

Responding to incidents of misuse

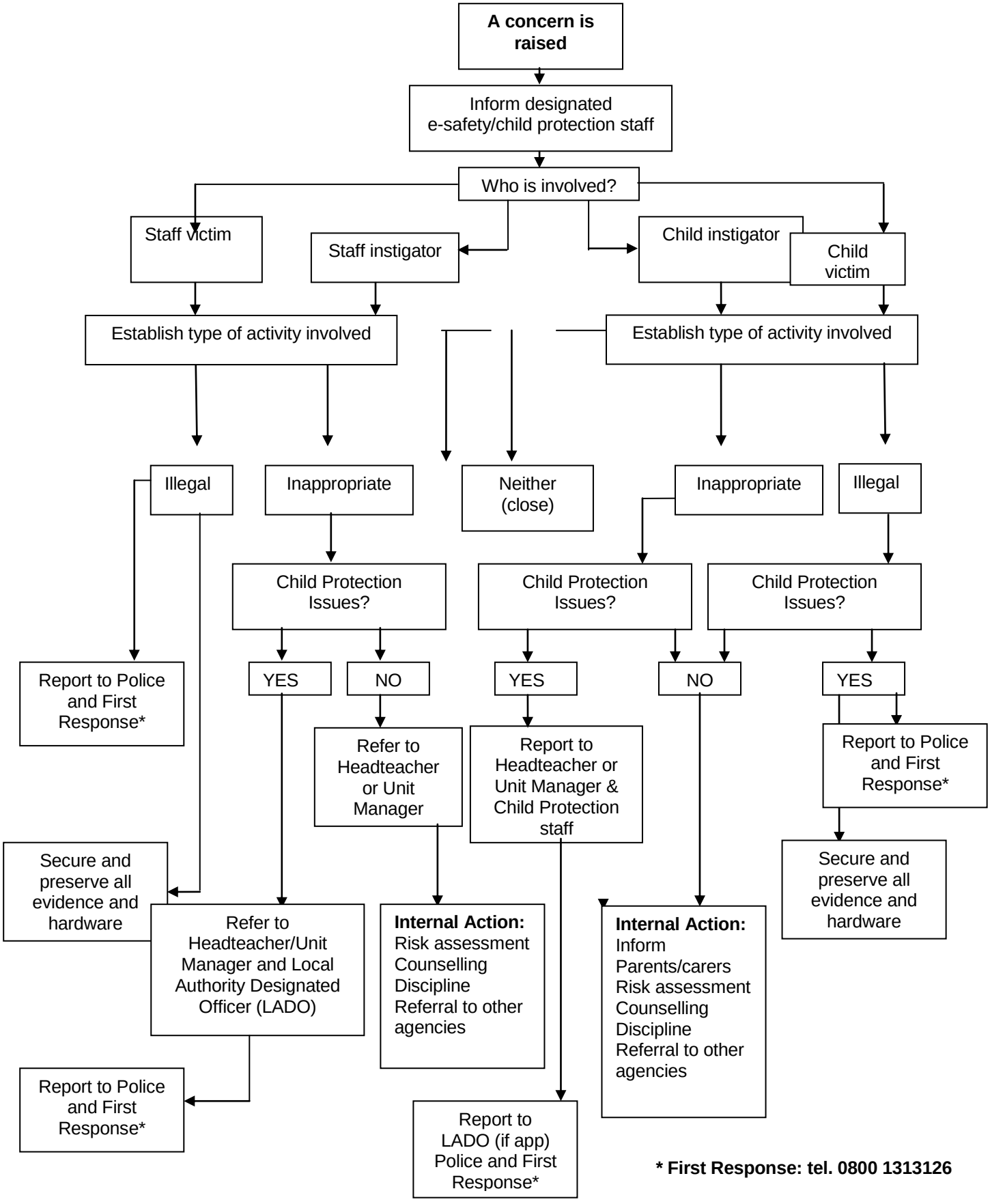
It is hoped that all members of the school community will be responsible users of I.C.T., who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are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

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 or materials

The flow chart from the Staffordshire Safeguarding Children's board, below and http://www.staffsscb.org.uk/professionals/esafety/e-SafetyToolkit/IncidentResponse/ will be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Staffordshire Local Safeguarding Children Board



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event, contact the Staffordshire Safeguarding Children's Board.

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 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:

Pupils — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Phase Leader / E-Safety Co-ordinator	Refer to Headteacher	Refer to Police	support staff for action re filtering / security	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 (see list in earlier section on unsuitable / inappropriate activities).			✓			✓	✓		
Unauthorised use of non-educational sites during lessons	✓	✓							
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓							
Unauthorised use of social networking / instant messaging / personal e-mail	N/A								
Unauthorised downloading or uploading of files		✓							
Allowing others to access school network by sharing username and passwords			✓						
Attempting to access or accessing the school network, using another student's			✓						

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

Staff	**Actions / Sanctions**							
Incidents:	Refer to Phase Leader	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Technical Support Staff for action	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).		✓						✓
Inappropriate personal use of the internet / social networking sites / instant messaging / personal e-mail		✓				✓		
Unauthorised downloading or uploading of files		✓				✓		
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		✓				✓		
Careless use of personal data eg holding or transferring data in an insecure manner		✓				✓		
Deliberate actions to breach data protection or network security rules		✓						✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓						✓
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓						✓
Using personal e-mail / social networking / instant messaging / text messaging to carrying out digital		✓						✓

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

Appendices

Appendices can be found on the following pages:

Parent / Carer Acceptable Use Policy Agreement

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people will have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school I.C.T. systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to I.C.T. to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to I.C.T. systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of I.C.T. – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and I.C.T. systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the I.C.T. systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed		Date	

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carer's Name	
Pupil Name	

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed		Date	

Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Pupil Acceptable Use Agreement.

Pupil Acceptable Use Policy Agreement

School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people will have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school I.C.T. systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to I.C.T. to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use of ICT

We use the school computers and Internet connection for learning.
These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any Web site, unless my teacher has already approved that site and I will not click into other sites, from this one, without permission.
- I understand that I should double check information I find on the internet as it may not always be reliable (correct).
- I understand that I should not copy images or words created by others and placed on the internet unless I have their permission. I know I must never pretend that this is my own work.
- On the network or learning platform, I will use only my own login and password, which I will keep secret.
- I will not look at, change or delete other people's files.
- I will not bring storage media (e.g. USB devices, CDROMS etc) to use in school without permission.
- I will only use the ICT suite and notebook computers for school and home learning.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail or using a discussion page, I will not give my home address or phone number, or arrange to meet anyone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet discussion forums unless given permission to do so by my teacher.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer and learning platform files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

- I will try to follow the 'THINK SMART' motto to help keep myself safe when using the internet (Key stage 1 will follow the 'THINK' rules and Key stage 2 will follow the 'SMART' rules).

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Name of Pupil			
Class			
Signed		Date	

Staff and Volunteer Acceptable Use Policy

School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school I.C.T. systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of I.C.T. in their everyday work.

The school will try to ensure that staff and volunteers will have good access to I.C.T. to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school I.C.T. systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the I.C.T. systems and other users. I recognise the value of the use of I.C.T. for enhancing learning and will ensure that pupils receive opportunities to gain from the use of I.C.T.. I will, where possible, educate the young people in my care in the safe use of I.C.T. and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the I.C.T. systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school I.C.T. systems (eg laptops, email, learning platform etc) in and out of school.
- I understand that the school I.C.T. systems are primarily intended for educational use and that I will only use the systems as set out in the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher

I will be professional in my communications and actions when using school I.C.T. systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / LP) it will not be possible to identify by name, or other personal information, those who are featured unless I have permission to do so.
- I will only use chat and social networking facilities on the learning platform in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will use it in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will ensure that I only use the schools email addresses on the school I.C.T. systems
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. .
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be transferred on a secure memory stick (pin coded)
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school I.C.T. equipment in school, but also applies to my use of school I.C.T. systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school I.C.T. systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

School Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the Staffordshire Learning Network (SLN) schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs
- be reported to a second responsible person (Headteacher) for authorisation

All users have a responsibility to report immediately to the System Manager, any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe will have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel will be filtered (or unfiltered) will report this in the first instance to the System Manager who will decide whether to make school level changes (as above). If it is felt that the site will be filtered (or unfiltered) at county level, the responsible person (Headteacher) will contact SLT with the URL.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement.

Monitoring will take place as follows:

- instigated by System Manager
- carried out on a regular basis (at least weekly)
- monitored using Securus monitoring solution
- recorded in log

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (Headteacher)
- E-Safety Governor / Governors Curriculum sub-committee
- Local Authority on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

School Password Security Policy

Introduction

The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user will be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school I.C.T. systems, including e-mail and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of I.C.T. Technician / I.C.T. Co-ordinator.

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by System Manager. Any changes carried out must be notified to the manager of the password security policy (above).

Users will change their passwords termly.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction

- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in I.C.T. and / or e-safety lessons
- through the Acceptable Use Agreement

Policy Statements
All users will have clearly defined access rights to school I.C.T. systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Curriculum Committee.

The following rules apply to the use of passwords:

- *passwords must be changed every 90 days*
- *the last four passwords cannot be re-used*
- *the password* will *be a minimum of 8 characters long and*
- *must include three of – uppercase character, lowercase character, number, special character*
- *the account* will *be "locked out" following six successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *requests for password changes* will *be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user* (requests will be authorised by a line manager for a request by a member of staff and by a member of staff for a request by a pupil)

The "administrator" passwords for the school I.C.T. system, used by the Network Manager must also be available to the Headteacher and kept in a secure place (e.g. school safe).

Audit / Monitoring / Reporting / Review
The responsible person (I.C.T. Coordinator) will ensure that full records are kept of:

- User ids and requests for password changes
- User log-ons

- Security incidents related to this policy

These will be reported to E-Safety Co-ordinator.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by the Curriculum Committee at regular intervals (termly). This policy will be regularly reviewed in response to changes in guidance and evidence gained from the logs.

School Personal Data Handling Policy

Introduction

Schools will do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (Becta – Good Practice in information handling in schools – keeping data secure, safe and legal – Sept 2008).

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it can not be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Fair Processing Code" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities

The school's Senior Risk Information Officer (SIRO) is Sarah Lewis and Jo Nickolls. They will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand :

- what information is held and for what purpose
- how information as been amended or added to over time
- who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Display equipment must be positioned so that the screen display is not visible to any unauthorised persons.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the "Fair Processing Notice"

Under the "Privacy Notice (previously known as Fair Process)" requirements in the Data Protection Act, the school will inform parents / carers of all pupils of the data they hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, DCSF, QCA, etc) to whom it may be passed. This fair processing notice will be passed to parents / carers through the school prospectus, newsletters, reports or a specific letter / communication and will be available on the learning platform. Parents / carers of young people who are new to the school will be provided with the fair processing notice through the school prospectus, newsletters, reports or a specific letter / communication and will be available on the learning platform.

PRIVACY NOTICE

Pupils in Schools, Alternative Provision and Pupil Referral Units and children in Early Years Settings

Privacy Notice - Data Protection Act 1998

We **(Churchfield C.E. (C) Primary School)** are the Data Controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information [1] and personal characteristics such as your ethnic group, special educational needs and any relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some of your information to the Local Authority and the Department for Education (DfE)

If you want to see a copy of the information we hold and share about you then please contact (Max Littlewood, office administrator).

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

http://www.staffordshire.gov.uk/education/yourdata/ and

[1] Attendance is not collected for pupils under 5 at Early Years Settings or Maintained Schools

http://www.teachernet.gov.uk/management/ims/datamanagement/privacynotices/pupilsdata/

http://www.teachernet.gov.uk/management/ims/datamanagement/privacynotices/pupilsdata/thirdpartyorgs/

If you are unable to access these websites, and need a hard copy, please contact the LA or DfE as follows:

- Information Governance Unit
  Law & Governance Directorate
  Staffordshire County Council
  1A Bailey Street
  Stafford
  ST17 4BG
  e-mail: foi@staffordshire.gov.uk

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT
  Website: www.education.gov.uk
  email: info@education.gsi.gov.uk
  Telephone: 0870 000 2288

(County template – update from Intranet annually)

Training & awareness

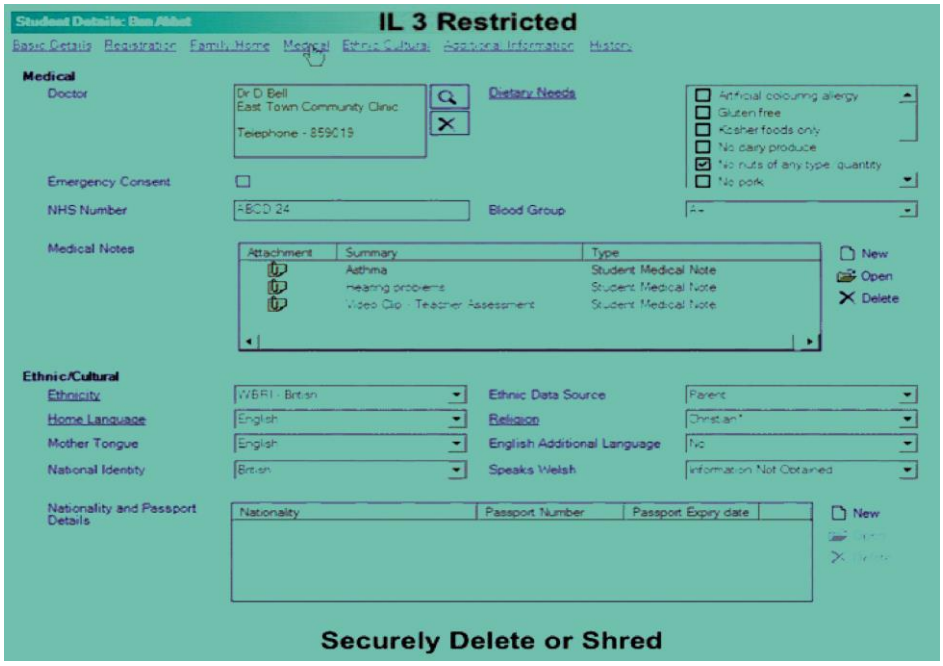
All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Identification of data

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

All documents (manual or digital) that contain protected data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer:



Impact levels are as follows:

- IL1–Not Protectively Marked (IL1–NPM)
- IL2–Protect
- IL3–Restricted
- IL4–Confidential

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data.

Release and destruction markings will be shown in the footer as follows:

[Release]	[Parties]	[Restrictions]	[Encrypt, Securely delete or shred]
The authority descriptor	The individuals or organisations the information may be released to	Descriptor tailored to the specific individual	How the document will be destroyed
Examples:			
Senior Information Risk Owner	School use only	No internet access No photos	Securely delete or shred
Teacher	Mother only	No information to father ASBO	Securely delete or shred

Secure Storage of and access to data

The school will ensure that I.C.T. systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and strong passwords which must be changed regularly (every 90 days). User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (ie owned by the users) must not be used.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests (i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject). Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location. Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care will be taken if data is taken or transferred to another country, particularly outside Europe, and advice will be taken from the local authority in this event. (N.B. to carry encrypted material is illegal in some countries)

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

***A Destruction Log will be kept of all data that is disposed of. The log will include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events will be archived and retained at evidential quality for seven years.

(****detailed guidance on audit logging in the Becta document "Good practice in information handling in schools - audit logging and incident handling - a guide for staff and contractors tasked with implementing data security")
The school has a policy for reporting, managing and recovering from information risk incidents, which establishes: *******

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Further reading

Teachernet – Data processing and sharing -
http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/
Office of the Information Commissioner website:
http://www.informationcommissioner.gov.uk
Office of the Information Commissioner – guidance notes: Access to pupil's information held by schools in England
Becta – Good Practice in information handling in schools – keeping data secure, safe and legal and it's four detailed appendices: (September 2008)
http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf
http://schools.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf
http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf
http://schools.becta.org.uk/upload-dir/downloads/audit_logging.pdf
http://schools.becta.org.uk/upload-dir/downloads/remote_access.pdf
Cabinet Office – Data handing procedures in Government – a final report (June 2008)
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

Legislation

Schools will be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e-safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-

commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person

harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes 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 Harrassment 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.

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.

Sexual 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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

E-Safety – A School Charter for Action

We are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of I.C.T., and follows agreed policies to minimise potential e-safety risks.

Our school community

Discusses, monitors and reviews our e-safety policy on a regular basis. Good practice suggests the policy will be reviewed annually or at most every two years. Churchfield have agreed to review this policy annually through Curriculum Committee.

Supports **staff** in the use of I.C.T. as an essential tool for enhancing learning and in the embedding of e-safety across the whole school curriculum.

Ensures that **pupils** are aware, through e-safety education, of the potential e-safety risks associated with the use of I.C.T. and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's e-safety policy.

Provides opportunities for **parents/carers** to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. The school will report back to parents / carers regarding e-safety concerns. Parents/carers in turn work with the school to uphold the e-safety policy.

Seeks to learn from e-safety good practice elsewhere and utilises the support of the **LA and relevant organisations** when appropriate.

Chair of Governors	Sean O'Meara
Headteacher	Jo Nickolls
Pupil Representative	Chair of School Council

Ideas for schools to consider

To assist schools in drawing up their e-safety policy, the school may wish to use the following prompts when determining and evaluating their policy, which are based on a document contained in the DCSF "Safe to Learn" Overview:
http://www.teachers.gov.uk/docbank/index.cfm?id=11907

Discuss, monitor and review

- Do we hold discussions on e-safety and its definition, involving staff, children and young people, governors and parents?
- Do we keep a record of the incidence of e-safety incidents, according to our agreed definition, and analyse it for patterns – people, places, groups, technologies?
- Do we ask ourselves what makes an e-safe school?
- What is our school doing to ensure that our children and young people do not feel vulnerable and are safe to learn, when engaged in online activities?
- Do we celebrate our successes and draw these to the attention of parents/carers and the wider community?

Support everyone in the school community to identify and respond

- Do we work with staff and outside agencies to identify all potential forms of e-safety incidents?
- Do we actively provide systematic opportunities for developing pupils' skills to develop safe online behaviour?
- Have we considered all the opportunities where this can be addressed – through the curriculum; through corridor displays; through assemblies; through the School Council; through peer support; and through the website and parents' evenings and newsletters?
- Do we ensure that there is support for vulnerable children and young people?
- Do we train all staff to be aware of potential e-safety issues and follow school policy and procedures on e-safety?
- Do our staff feel adequately supported to be able to respond to and manage e-safety related incidents?

Ensure that children and young people are aware of how and to whom e-safety incidents will be reported and understand that all e-safety concerns will be dealt with sensitively and effectively

- Do we acknowledge and learn from the high level of skills and knowledge of children and young people in the use of new technologies? (often referred to as the "digital natives")
- Do we regularly canvass children and young people's views on the extent and nature of e-safety issues?

- Do we ensure that young people know how to express worries and anxieties about e-safety?
- Do we ensure that all children and young people are aware of the range of sanctions which may be applied against those involved in e-safety misuse?
- Do we involve children and young people in e-safety campaigns in school?
- Do we demonstrate that we are aware of the power of peer support? Have we created and publicised schemes of peer mentoring or counselling; buddying or mediation, for example?
- Do we include the phone numbers of help-lines in the school's student planners?
- Have we made children and young people aware of "how to report abuse"?
- Do we have an e-safety notice board?
- How else do we bring e-safety messages to children and young people's attention?
- What role does our School Council already play in our e-safety work? How might that involvement be enhanced?
- Do we offer sufficient support to children and young people who have been involved in e-safety incidents?
- Do we work with children and young people who have been involved, or may be seen as being at risk?

Ensure that parents/carers are aware of e-safety issues and that those expressing concerns have them taken seriously

- Do we work with parents and the local community to address issues beyond the school gates that give rise to e-safety issues? – particularly with regard to the possible lack of filtering and monitoring of internet access by children and young people out of school and with regard to cyber-bullying incidents
- Do parents know whom to contact if they are worried about e-safety issues?
- Do parents know about our complaints procedure and how to use it effectively?

Learn from effective e-safety work elsewhere and establish effective collaboration

- Have we invited colleagues from a school with effective e-safety policies and practice to talk to our staff?
- Have we involved local authority staff or other local / regional experts in any way?
- Do we have an established link with the police?