



Sileby Redlands Community Primary School e-Safety Policy

At Sileby Redlands Community Primary School we will develop the learning environment to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they develop their personalised learning, in line with our school's vision.



Contents

Contents	1
Why is Internet Use Important?	2
How does Internet Use Benefit Education?	2
How can Internet Use Enhance Learning?	2
Authorised Internet Access	3
World Wide Web	3
E-Safety	3
School e-Safety Policy	4
Good Habits	4
Governors:	4
Headteacher and Senior Leaders:	5
E-Safety Officer:	5
Network Manager:	5
Teaching and Support Staff are responsible for ensuring that:	6
Designated person for child protection	7
Pupils:	7
Parents / Carers:	7
Community Users:	8
Policy Statements:	8
Education – pupils	8
Education – parents / carers:	8
Technical – infrastructure / equipment, filtering and monitoring:	9
Curriculum:	11
Use of digital and video images - Photographic, Video:	11
Use of e-mail:	12
Use of Social Networking:	12
Data Protection:	13
Staff Responsibilities:	13
Communications:	14
When using communication technologies the school considers the following as good practice:	15
Unsuitable / inappropriate activities:	15
Responding to incidents of misuse:	17
Handling e-safety Complaints:	17
Communication of Policy	19
Pupils	19
Staff	19
Parents	19
Appendices	22
Pupil Acceptable Use Policy Agreement	23
Pupil Acceptable Use Agreement Form	26
Staff (and Volunteer) Acceptable Use Policy Agreement	27
Acceptable Use Policy Agreement	28
Parent / Carer Acceptable Use Policy Agreement	31
Use of Digital / Video Images	33
School Filtering Policy	34
School Password Security Policy	36
Policy Statements	37
Legislation	38



Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet in and outside of school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Pupils will begin to use the school's Learning Platform (VLE) as a secure online learning environment both in school and at home.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.



- Pupils will be educated in the effective use of the Internet in research, including the skills of key word searching, knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All pupils will be asked to read and sign an age appropriate 'Acceptable ICT Use Agreement'.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- Sileby Redlands Community Primary School use a "filtered" Internet Service, which will minimise the chances of pupils encountering undesirable material. The school will normally only allow children to use the Internet when there is a responsible adult present to supervise. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils. Teachers will have access to pupils' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety officer or network manager.
- The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

E-Safety

E-Safety encompasses Internet technologies and electronic communications such as iPads, mobile phones and wireless technology. It highlights the need to educate our pupils about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Sileby Redlands Community Primary School's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.



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

The Education and Inspections Act 2006 empowers Head teachers, 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.

School e-Safety Policy

Our e-Safety Policy has been written by the school, building on accepted good practice from the likes of UK Safer Internet Centre, 360 Safe and CEOP. It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be overviewed annually, and reviewed every three years. This policy will next be reviewed in 2016.

Good Habits

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

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Leicestershire County Council including the effective management of content filtering.
- National Education Network standards and specifications.

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.



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 Officer.
- The Headteacher is responsible for ensuring that the e-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as is relevant.
- The Head teacher will ensure 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.
- The Senior Leadership Team will receive regular monitoring reports from the e-Safety Officer.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Officer:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / 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.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team

Network Manager:

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in 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 periodically changed



- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he keeps 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 monitoring software and systems are implemented and updated as agreed in school policies

Teaching and Support Staff are responsible for ensuring 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 Agreement
- they report any suspected misuse or problem to the e-Safety Officer
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should 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 lessons where internet use is pre-planned pupils should 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 (including making use of the opportunity to reinforce e-safety messages, acceptable use and the inclusion of safe and responsible use of the internet within the curriculum.



Designated person for child protection

The designated person/s should be 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

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, 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 should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should 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 / 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 ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy



- accessing the school website / VLE / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users:

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

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 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 should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Pupils should 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 should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers:

Many parents and carers have only 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 of the children's on-line experiences. Parents often either underestimate or do not realise how often children 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
- Parent information sessions
- Learning Together sessions

Technical – infrastructure / equipment, filtering and monitoring:

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority e-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager.
- All users will be provided with a username and password. Children in Key Stage 2 will have their own username and password for the VLE with the capability to alter the password to one of their choosing. The e safety officer will have the ability to reset passwords if misplaced.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in the school safe.
- Users will be made responsible 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.



- 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.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and e-Safety Officer. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the e-Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager or e-Safety Officer. The log is to be found in the Staff Room
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, 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” (eg supply or trainee teachers or visitors) onto the school system. In the case of Infrastructure Engineers the Master/Administrator password will be taken from the school safe by the e-safety officer or Head Teacher and given so that essential work may be carried out. The password will then be reset by the Network Manager at the next visit to school.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school. (see School Personal Data Policy Template in the appendix for further detail)
- An agreed policy is in place that **forbids** staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices. (see School Personal Data Policy Template in the appendix for further detail)
- The school infrastructure and individual workstations are protected by up to date virus software.



- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

Curriculum:

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that pupils should 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, eg using search engines, staff should 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager and e-Safety Officer can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- Pupils should 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:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg 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 should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.**
- Care should 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
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Use of e-mail:

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

Use of Social Networking:

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.



- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

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 Responsibilities:

- 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, cloud device or any other removable media:
 - the data must be encrypted and password protected
 - the device must be password protected (many memory sticks / cards and other mobile devices cannot 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 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:

Communication technologies	Staff and other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with 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 personal devices				✓				✓
Use of hand held devices eg PDAs, PSPs		✓					✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓		✓		
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs [educational]	✓					✓		



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

- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities:

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as listed in the following table:



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					X
	Promotion or conduct of illegal acts, eg under child protection, obscenity, computer misuse and fraud legislation					X
	Adult material that potentially breaches the Obscene Publications Act in the UK					X
	Criminally racist material in UK					X
	Pornography				X	
	Promotion of any type of discrimination				X	
	Promotion of racial or religious hatred				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business				X		
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publishing confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files				X		
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				X		
On-line gaming (educational)	X					
On-line gaming (non educational)		X				
On-line gambling				X		
On-line shopping/commerce			X			
File sharing			X			
Use of social networking sites				X		
Use of video broadcasting eg Youtube			X			



Responding to incidents of misuse:

It is hoped that all members of the 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:

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

- 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 below should 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.

Handling e-safety Complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Head Teacher.

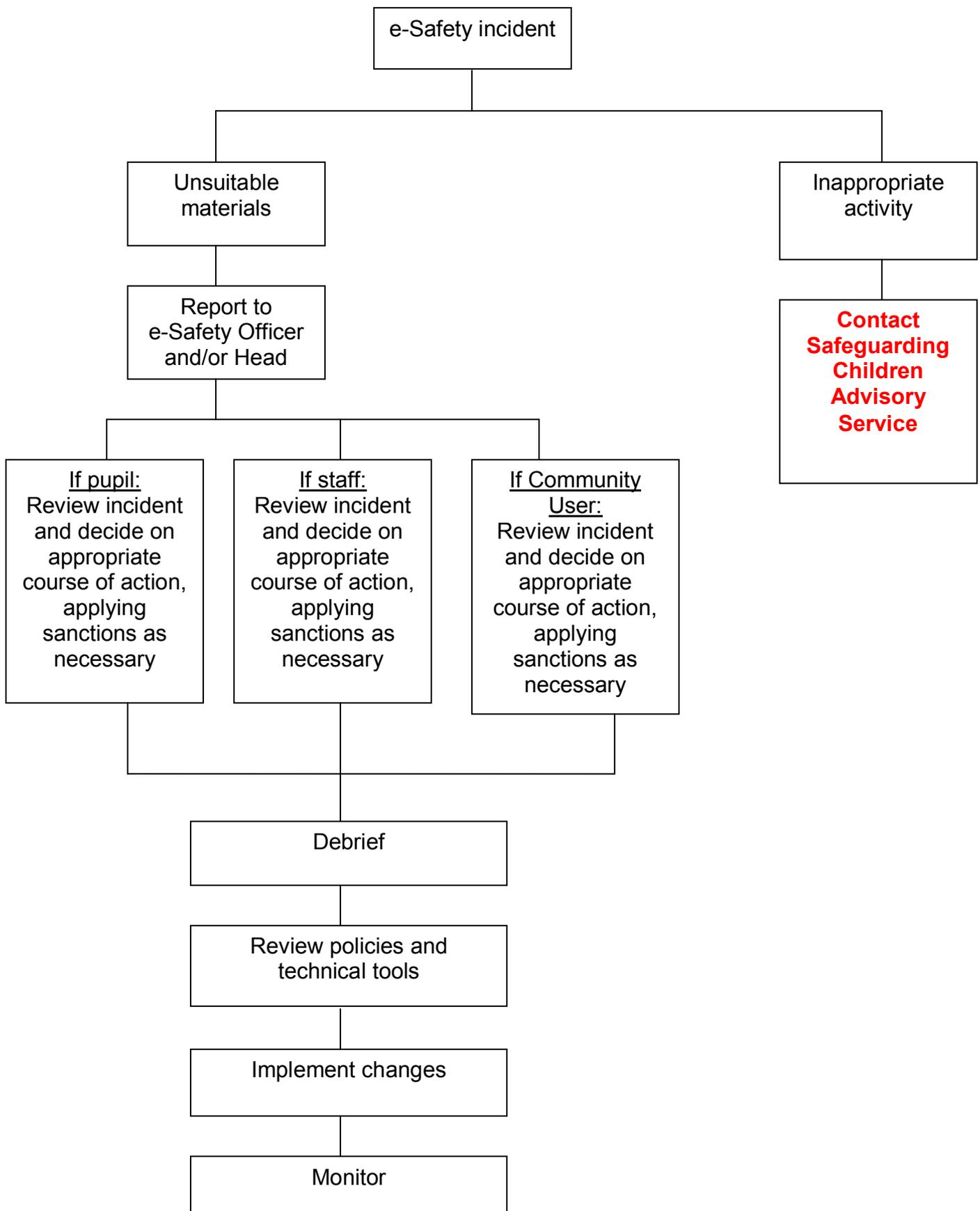
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure.

- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.



Flowchart for responding to e-Safety incidents at Sileby Redlands Community Primary School Adapted from Becta – E-safety 2005





Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be educated in e-Safety.
- Pupils will be required to take home and sign in conjunction with their parents a 'Pupil Acceptable Use Agreement'.

Staff

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

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Parent's will sign with their child the 'Pupil Acceptable Use Agreement'.
- Learning Together workshops will be run for parents to make them aware of e-safety issues both at school and at home.
- Information will be provided to parents offering guidance on promoting e-safety messages in home use of ICT.

Community Resource Users

- Users of the Sileby Redlands Community Primary School ICT must sign an 'Acceptable Use Agreement' prior to accessing School resources.



Pupils	Actions/Sanctions							
	Refer to class teacher	Refer to Head Teacher	Refer to Police	Refer to network manager	Inform parents/carers	Removal of network/internet access/rights	Warning	Further sanction eg exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in User Actions table)		X	X		X			
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone/digital camera/other hand held device	X	X			X		X	
Unauthorised use of social networking/instant messaging/personal e-mail	X	X			X		X	
Unauthorised downloading or uploading of files	X	X		X	X		X	
Allowing others to access school network by sharing username and passwords	X				X		X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X			X		X	
Corrupting or destroying the data of other users	X	X			X		X	
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach of integrity of the ethos of the school	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Receipt or transmission of materials that infringes the copyright of another person or infringes the Data Protection Act	X	X			X		X	



Staff	Actions/Sanctions							
	Refer to line manager	Refer to Head Teacher	Refer to Police	Refer to network manager	Refer to LA	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in User Actions table)	X	X		X	X	X		
Excessive or inappropriate personal use of the Internet/social networking sites/instant messaging/personal e-mail	X							
Unauthorised downloading or uploading of files		X		X				
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X				X		X
Careless use of personal data eg holding or transferring data in an insecure manner	X							
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X				X		X
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature		X			X			X
Using personal e-mail/social networking/instant messaging/text messaging to carry out digital communications with pupils		X			X			X
Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the school into disrepute or breach of integrity of the ethos of the school		X						
Using proxy sites or other means to subvert the school's filtering system	X	X		X		X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X				
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X		X	X
Breach copyright or licensing regulations	X	X		X		X		
Continued infringements of the above, following previous warnings or sanctions			X		X		X	X



Appendices

Can be found on the following pages:

• Pupil Acceptable Usage Policy template	26
• Staff and Volunteers Acceptable Usage Policy template	30
• Parents / Carers Acceptable Usage Policy Agreement template	33
• Use of digital/video images parental consent form	35
• School Filtering Policy template	36
• School Password Security Policy template	38
• Legislation	41
• Links to other organisations and documents	44
• Resources	46
• ‘Think Then Click’ Internet Rules	47



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 should 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 ICT 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 ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.



- 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 use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- I will not steal, disable or cause any damage to school equipment, or the equipment belonging to others.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school **ONLY** when I have permission **AND AFTER** it has been tested for viruses. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- 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.
- I will only use chat and social networking sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.



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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.



Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

My child and I have read through and understood the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, PDAs cameras etc
- I use my own equipment out of school in a way that is related to me being a member of Sileby Community Primary School eg communicating with other members of the school, accessing school email, website VLE etc.

Name of pupil

Pupil signature

Year Group

Signed (parent/carer)

Date



Staff (and Volunteer) 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. 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 ICT 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 ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT 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 ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT 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 ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within 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 appropriate person.

I will be professional in my communications and actions when using school ICT 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.
- Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites 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 follow the rules set out in this agreement, 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 take greater care when using personal email addresses on the school ICT systems and will not download any programs from it nor open any inappropriate material that may have been sent to it by others.
- 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 ensure that my data is regularly backed up, in accordance with relevant school policies, remembering that data in My Documents when logged into the school server is backed up but that other personal folders on laptops are not backed up by the school system and these are my own responsibility to securely back up.
- 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 this School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- 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 ICT equipment in school, but also applies to my use of school ICT 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 ICT 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



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 should 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 ICT 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 ICT 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 pupil, I give permission for my son / daughter to have access to the internet and to ICT 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 ICT – 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 ICT 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 ICT 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

e



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 cannot 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. Please note that non return of this form will be taken by the school as implicit permission. However, we do ask that forms are completed and returned for all instances.

I have read the Acceptable Use of Digital / Video Images and have circled below how I wish images of my child to be used.

Parent's Consent for Web Publication of Work and Photographs

Images of _____ (name of child) may be published in the following ways:		
On the school website	Yes	No
On the secure learning platform	Yes	No
In the press	Yes	No
For displays within school	Yes	No
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.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network. 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 (e-Safety Officer):**
- be reported to and authorised by a second responsible person prior to changes being made

All users have a responsibility to report immediately to e-Safety Officer any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should 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
- 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 should be filtered (or unfiltered) should report this in the first instance to the e-Safety Officer who will decide whether to make school level



changes. If it is felt that the site should be filtered (or unfiltered) the Network Manager should alter the filter settings to block this content.

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:

Audit / Reporting

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

- the second responsible person (insert title)
- E-Safety Committee
- Governors committee

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).



School Password Security Policy

Introduction

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible. Each class has their own username and password.

Students and staff are responsible for keeping their own log in details for the VLE private and confidential.

Responsibilities

The management of the password security policy will be the responsibility of the ICT Subject Leader.

All users (adults and students) will have responsibility for the security of their username and password and 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 the Network Manager or VLE administrators. Any changes carried out must be notified to the manager of the password security policy.

Staff Users should change their passwords every term or at minimum every school year. Any suspected breach, particularly where someone else may know a users password, must be reported and the user **MUST** change their password immediately.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

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

- in ICT and / or e-safety lessons
- through the Acceptable Use Agreement



Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager.

All users will be provided with a username and password by the Network Manager or VLE Administrators who will keep an up to date record of users and their usernames. Users will be required to change their password periodically or immediately if a breach of security is suspected

The following rules apply to the use of passwords with the VLE:

- staff user passwords must be changed every term or at minimum every school year.
- 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)
- passwords can be changed by the individual user by going through the 'Settings' option.

The "master / administrator" passwords for the school ICT system, used by the Network Manager is also available to the Headteacher and kept in the school safe. This/these administrator level passwords must be treated at all times with the utmost confidentiality and NOT passed onto anyone other than the Head Teacher or Network Manager. Any breach must be flagged to Head Teacher and Network manager immediately for further action to be taken and for those passwords compromised to be changed.



Legislation

Schools should 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 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.

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 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 students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.



Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

SOUTH WEST GRID FOR LEARNING:

“SWGfL Safe” - <http://www.swgfl.org.uk/staying-safe>

Child Exploitation and Online Protection Centre (CEOP)

<http://www.ceop.gov.uk/>

ThinkUKnow

<http://www.thinkuknow.co.uk/>

CHILDNET

<http://www.childnet-int.org/>

INSAFE

<http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

BYRON REVIEW (“Safer Children in a Digital World”)

http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/27_03_08byronreview.pdf

Developing whole school policies to support effective practice:

http://www.hcvs.org.uk/EN/store/Policies/CYP_e-safety_guide_kids.pdf

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:

<http://www.mmiweb.org.uk/publications/ict/esafetyks1and2.pdf>

“Safeguarding Children in a Digital World”

<http://webarchive.nationalarchives.gov.uk/20101102103654/publications.becta.org.uk//display.cf m?resID=35446>

KENT NGfL

<http://www.kented.org.uk/ngfl/ict/safety.htm>

NORTHERN GRID

<http://www.northerngrid.org/index.php/esafety-and-security>

NATIONAL EDUCATION NETWORK

NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

CYBER-BULLYING

DFE - Cyberbullying guidance

<http://www.kidscape.org.uk/cyberbullying/cyberbullyingdcsf.html>

Teachernet “Safe to Learn – embedding anti-bullying work in schools”

<http://www.playfieldinstitute.co.uk/information/pdfs/publications/bullying/SafeToLearn.pdf>

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>



East Sussex Council – Cyberbullying - A Guide for Schools:

<https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx>

SOCIAL NETWORKING

Home Office Task Force - Social Networking Guidance -

<http://www.sheffield.ac.uk/content/1/c6/10/72/33/2005-Guidance-Social-Networking.pdf>

Digizen – “Young People and Social Networking Services”:

<http://www.digizen.org/socialnetworking/>

Ofcom Report:

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

MOBILE TECHNOLOGIES

“How mobile phones help learning in secondary schools”:

archive.teachfind.com/becta/research.becta.org.../lsri_report.pdf

DATA PROTECTION AND INFORMATION HANDLING

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

BECTA - Data Protection:

<http://webarchive.nationalarchives.gov.uk/20081105151713/foi.becta.org.uk/display.cfm?cfid=1170520&cftoken=75353a58ed02e72a-6d3b4bbc-0a00-454d-edba9b0745a9b559&page=1759>

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:

<http://parents.vodafone.com/about>



Resources

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the “SWGfL Safe” website:

<http://www.swgfl.org.uk/staying-safe>

Links to other resource providers:

Kidsmart: <http://www.kidsmart.org.uk/default.aspx>

Know It All - <http://www.childnet-int.org/kia/>

Cybersmart - <http://www.cybersmartcurriculum.org/home/>

NCH - <http://www.stoptextbully.com/>

Chatdanger - <http://www.chatdanger.com/>

Internet Watch Foundation: <http://www.iwf.org.uk/>

Digizen – cyber-bullying films: <http://www.digizen.org/cyberbullying/film.aspx>



Think then Click



e-Safety rules for Key Stage One

These rules help us to stay safe on the Internet

- *We only use the Internet when an adult is with us.*
- *We can click on the buttons or links when we know what they do.*
- *We can search the Internet with an adult.*
- *We always ask if we get lost on the Internet.*
- *We can send and open emails together.*
- *We can write polite and friendly emails to people that we know.*





Think then Click

e-Safety Rules for Key Stage 2



- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

