

Draft Flow Chart of Roles and Responsibilities for E-Safety

Role	Responsibility	Area 1	Area 2	Area 3	Area 4
Director of Children's Services	Personally liable, responsible and accountable for safeguarding all young people within the Local Authority	Does the LA have robust systems and CRB checked personnel who are responsible for creating, monitoring and reporting of all aspects of Electronic Communications?	Does the DCS receive regular reports on these processes, infringements, violations and other issues of misuse together with actions taken to resolve?	Are there stringent reporting systems to report and deal with illegal or misuse of systems? Are there clear sanctions laid out for misuse?	Is there an LA AUP? Has this been shared with all employees and signed by them?
LA Head of Education or corporate ICT	Responsible for identifying systems for protecting users from abuse of misuse Responsible for setting up systems that protect and catch misuse Responsible for disseminating policy to all LA users and to schools Responsible for high level monitoring at system level and at user level where users directly access the LA system	Is the ISP used a signed up member of the Internet Watch Foundation, applying their rules? Does the level of global filtering protect all users from sites which block racism, drugs, violence, weapons, pornography, hatred?	Are there global anti-virus and anti-spam systems? Are these updated frequently and applied to all systems? Do firewalls protect from denial of service attacks etc?	How is the system monitored for traffic use and site access? What reporting tools are available to track log usage? How are global or local proxy servers deployed? How are these managed and monitored?	How are passwords deployed? What agreed protocols are in place for password management? What checks are done to see if these are applied and used?

Role	Responsibility	Area 1	Area 2	Area 3	Area 4
	Responsible for reporting abuse of misuse using approved LA channels				
Head Teacher	Responsible for ensuring safety and protection of all members of staff, learners and visitors within an E Environment	<p>Is there an E-Safety Committee? What has it agreed as acceptable usage for all? Is the AUP a living working document? Has it been signed up to by all? Are there clear sanctions for misuse? Is the head confident that there are robust technical systems in place to ensure safe use? How is the head, the SMT and the E-Safety committee involved in receiving and reacting to reports of misuse?</p>	<p>Who has overall control of the school network, its accessibility and its protection? How does the head and the E-Safety Committee know that these systems are robust and applied?</p>	<p>Does the school enforce a stringent password and username policy?</p>	
Head of ICT	Responsible for ensuring that the school network is	<p>Network security: Servers should be protected</p>	<p>Filtering policies should be applied to all users as laid down in</p>	<p>All staff who use the system should be trained in acceptable</p>	<p>Regular reports should be provided to the E-</p>

Role	Responsibility	Area 1	Area 2	Area 3	Area 4
	<p>secure, not open to misuse or malicious attack</p> <p>Responsible for ensuring the school password policy is up to date and enforced</p> <p>Responsible for ensuring that the school filtering policy is applied and updated on a regular basis</p>		<p>the school's AUP CachePilots or proxy servers should be applied and all internet usage directed through these.</p> <p>Logs should be monitored either remotely – preferably – or manually on a regular basis to check for misuse or infringements of the AUP (training may be required for this)</p>	<p>use and able to report accidental or deliberate incidents.</p>	<p>Safety committee on inappropriate use and also on the effectiveness of the system</p>
School Technician or Network Manager	<p>Responsible to the head of ICT and the E-Safety Committee for following procedures.</p> <p>Responsible for reporting evidence of misuse but not responsible for tracking misuse</p>	<p>Desktops should be locked down</p> <p>User areas should be set up and password protected</p> <p>Passwords should be enforced</p> <p>Wireless access should be secure and encrypted.</p>	<p>Some of the above may apply depending on circumstances</p>	<p>Need to ensure that “guest accounts” are set up for visitors for an agreed time and then disactivated.</p>	<p>Need to understand the technical issues related to maintaining evidence in cases of serious infringement</p>
Staff Development Officer	<p>Responsible for understanding all</p>	<p>Needs to attend high level training and</p>	<p>Needs to establish a rolling programme of</p>	<p>Should provide awareness raising</p>	

Role	Responsibility	Area 1	Area 2	Area 3	Area 4
	aspects of E-Safety at macro level Responsible for sourcing appropriate training so that all users understand the benefits and potential hazards of the system	awareness raising to understand the issues regarding to e-safety. This will almost certainly need to be done outside the school.	in-service for staff, to ensure that they understand issues and are able to apply safe usage to all their lessons.	events for governors and parents	
Class teacher	Responsible for ensuring that pupils understand and follow the school's acceptable use policy. Responsible for monitoring ICT activity during lessons. Responsible for reporting any suspected misuse or problem relating to the school system.	E-Safety issues should be embedded into all aspects of curriculum work which use ICT.	Needs to liaise with school network manager and head of ICT to ensure that appropriate sites are pre-cached and available for each lesson. These should be included into medium and short term planning.	Need to ensure that students have good understanding of research skills and the need to avoid plagiarism. Need to ensure students understand how to reference source material appropriately.	
Pupils	Responsible for using the school system in accordance with the school's AUP. Responsible for reporting any accidental access to	Need to understand and sign AUP Need to be aware of sanctions for misuse.	Need to understand reasons for not copying directly or indirectly and internet based material without acknowledging source.	Need to understand how to report abuse, misuse or access to inappropriate materials	

Role	Responsibility	Area 1	Area 2	Area 3	Area 4
	inappropriate material found				
Parents/Carers	Responsible for ensuring that their children understand the need to use the internet in an appropriate way. Responsible for endorsing the school's AUP. Responsible for understanding what their children are using the internet for at home.	Parents need to countersign the school's AUP with their child.	They need to understand the need for an AUP – for their child's protection and for the protection of others – the school should assist with this through awareness raising sessions.	Parents should have access to materials – printed and online which can help them to understand how to ensure their child is safe on the internet at home.	