

E-Safety Audit – Secondary and Middle Schools



This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CFE guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both students and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for students?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access (e.g. the Kent Community Network).	Y/N
Has the school filtering policy has been approved by SMT?	Y/N
Has an ICT security audit has been initiated by SMT, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y/N
Have appropriate members of staff attended training on the KCN filtering system?	Y/N

e-Safety Policy Guidance

www.kenttustweb.org.uk?esafety

Becta e-Safety

www.becta.org.uk/schools/esafety



Schools ICT Security Policy

The integrity of the wide area network depends on the security policy implemented by each connected school, as well as central policies and security systems. The security policy below has been discussed widely with schools and all schools joining the KCN are required to agree to implement this policy.

Policy and Management:

- A senior manager will take overall responsibility for IS Security and appoint an IS Security Officer for the school.
- The school must have a current e-Safety policy. Pupils and staff must agree to comply with the rules for responsible Internet use, which should be prominently displayed. (See www.kenttrustweb.org.uk?esafety)
- The filtering software records Internet use for every user, as part of the strategy to prevent access to inappropriate materials. Access to this monitoring information should be authorized at senior level and staff given access supervised to ensure reasonable use.
- Network and Internet use is covered by legislation. The school will make users aware of relevant legislation including that covering Data Protection and Copyright.

Systems Implementation:

- IS Security Officer must approve all equipment connected to the network, software installed and any connections to external networks.
- There must be a policy on the availability to users of inappropriate executable files.
- An approved and current virus checker must be installed on workstations and servers.

Good practice:

- Good log-in and password practice must be observed by all users.
- Good network management practice including secure network equipment location, logging-out after use and sound backup and recovery strategies will be implemented.
- An Internet access filtering system appropriate to school use is implemented either centrally or at school level. The Kent Community Network supplies such a system.
- The waste of system resources for non-educational reasons needs to be minimized.
- All external facing services should reside in a DMZ network.

School:

Signed: (headteacher)