# e-Safety Policy Checklist

**03 March 2010**

**Please note**: this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice.

This document is a checklist of questions for institutions to consider when updating or framing a new e-safety policy. It serves as a quick reference guide. An effective policy may protect the college from legal challenge, relating to use of ICT and assist colleges to meet their statutory obligations. It is recommended that colleges carry out an audit of existing e-safety strategies prior to using this checklist.

1. Does your institution's policy reflect the views of all stakeholders, including learners, from your college community?
2. Are all staff and students made aware of their rights and responsibilities prior to using ICT at the institution?
3. Is the scope of the policy clear? (e.g. do provisions cover use of ICT by volunteers, supply staff, community users, carers, visitors)
4. Does the policy govern in what circumstances (e.g. e-learning settings, use of mobile technologies) it will apply?
5. Is the policy easily understood by all users of ICT? (e.g. of suitable length, language and tone?)
6. Does your e-safety policy link to other college policies (e.g. acceptable use, e-security, web 2.0, anti bullying and child protection policies) already in place?
7. Is reference made to e-security measures for secure access and transference of encrypted data off site?
8. Does your institution's policy provide specific instructions for users on how they can report any offending material, and to whom?
9. Does the policy include clear e-safety handling procedures (e.g. in a flow chart) listing unacceptable/illegal behaviours, including sanctions and reporting procedures?
10. Does the policy contain procedures for assessing risk, escalating an incident, engaging multi agency support?
11. Is there a list of further sources of information, guidance and support included?
12. Does the policy make provision for a planned programme of dissemination and training on e-safety issues for all users?
13. Does the policy include a procedure for measuring and monitoring its impact?
14. Does your institution's policy provide a clear procedure for review (e.g. annually) in line with emerging technologies and web based resources?