



e-Safety... *Does your School meet Government Guidelines?*

Tel: 01256 301900
email: sales@reacttechnologies.com

Under the latest Government guidelines, every school has a responsibility to safeguard their pupils and minimise the risk of serious abuse. This includes measures to prevent students accessing inappropriate Internet content, cyber-bullying, self-harm, harmful or racist behaviour and predator grooming.

Whole-school responsibilities


Our integrated technology solutions encompass all IT aspects of the e-safety directive. Encompassing Network Access Control, Military grade Firewalls and Applications to monitor and control the usage of the computers in your school and alert you when a pupil puts themselves or others at risk.

The Internet has become an integral part of children's lives, enabling them to undertake research for school projects, talk to their friends and access information from around the world. Increasing provision of the Internet in and out of schools brings with it the need to ensure that learners are safe.

e-safety is aimed at encouraging children to act more responsibly and therefore create a better environment for learning.

"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 schools are bound. A framework of e-safety, or acceptable use policies (AUPs) can help to ensure safe and appropriate use. The development and implementation of such strategies should involve all the stakeholders in a child's education from the Head Teacher and governors to the senior management team and classroom teachers, support staff, parents, and the pupils themselves".

Quote from "Becta"

 **Safety... Every Child Matters**



REACTtechnologies.com



e-Safety... *Does your School meet Government Guidelines?*

Tel: 01256 301900
email: sales@reacttechnologies.com

Usage Monitoring and Control

Thousands of proxy bypass sites exist, which allow your students to avoid your blocking software and give unrestricted access to banned websites and chat rooms

- Detect when proxy bypass sites have been used
- Stop downloads of obscene or offensive content
- Get an early warning of predator grooming
- Know when pupils are planning to meet people they don't know
- Take appropriate action quickly
- Strengthen your pastoral care
- Curb personal website use
- Ensure ICT activity is on-task
- Control access to computer programs
- Encourage responsible ICT behaviour and enforce AUP
- Teach pupils how to act responsibly and safely online

By capturing evidence of any misuse, we can empower teaching staff. Incidents are dealt with outside the classroom and disruptive classroom behaviour reduced.

Network Access Control

User Identity and Authorization via a single endpoint policy compliance system, capable of virus protection and remediation with dynamic enforcement, over a wired or wireless network, or remote connection.

Supporting pre and post connect end point analysis, posture checking and able to self remediate Operating System Patches, Hot fixes, antivirus definitions, as well as client specific software.

User platform agnostic so can control any MAC, PC or Linux device.

Per User State Full Firewall

ICSA-Certified identity aware government approved Firewalls which enable granular differentiated access rights by user or device type(s).

Policy & Role based access control ensures compliance with approved security policies and permits templates to be applied based on individual rights or group membership.

Stateful flow classification enables identification of application flows for special treatment, such as QoS for Voice or Video.

