Securus Schools Computer Monitoring UK

Type of intervention

Online

Target group/s, level/s of prevention and sub-group/s:

Situations / Places	Schools and other organisations working with children and young people, Internet/Online | Online/App | Internet Specific Interventions | English

Target population

Schools and other educational establishments.

Delivery organisation

Securus Software Ltd. UK.

Mode and context of delivery

Securus is e-Safety software which examines and monitors computers linked into a school network. It looks for inappropriate words, phrases and images using a selection of libraries which enable the recognition of these items. Results are monitored by teaching staff who can then respond to concerning situations and take appropriate action.

Level/Nature of staff expertise required

Monitoring staff are teaching staff with knowledge of issues affecting children. They need to be proficient in the use of computers.

Intensity/extent of engagement with target group(s)

Schools can decide for how long they use the software.

Description of intervention

Once installed on computers and laptops, Securus monitors for anything inappropriate, either written or appearing as images. It covers both online and offline applications, including Microsoft Word and PowerPoint, even if content is not saved or it is deleted. It also covers all internet applications, including websites, email, Facebook, Twitter, MSN and chatrooms. Securus monitors inappropriate or concerning images or text, including words, phrases, slang and text speak. It can be used to monitor the following potential issues:

- online grooming and child abuse/exploitation
- cyberbullying
- explicit images
- depression, self-harm and suicide
- racial, homophobic and religious harassment
- use of drugs or weapons
- attempts to use a proxy bypass to access restricted sites

The software has two key components; a physical, secure server appliance and client software that is installed on all computers, laptops or remote devices in the school, that are to be included in the monitoring. The server provides the central monitoring and control database and receives data from the client software. The client software monitors the user's computer for prohibited words, phrases and images regardless of their source, whether online (e.g. chat rooms, websites, emails and any other online resource) or offline (e.g. Microsoft Office programmes, CD-ROMs, USB memory sticks). Any text appearing on the screen is scanned for prohibited words and phrases, held on custom libraries on the secure server.

If the client software detects a match with a word or phrase in any active libraries, it takes a snapshot of the computer screen at the time of the event and records it, together with the user name, computer name, date and time, all of which is then transmitted to the secure server. The software also alerts the people monitoring to any access to 'proxy Anonymiser' sites that could be used to bypass or defeat traditional security such as internet filtering and blocking solutions. In addition, an Image Analysis engine detects potentially concerning images. Those who manage these 'violations' can then log in to the server from a computer with internet access, regardless of their location to review the screenshots. All servers are physically tamper-proof and cannot be edited, altered or deleted, even during transmission of data.

Evaluation

No evaluation data available.

References

www.securus-software.com/securus-education/

Contact details

Securus Software Ltd
Address: Claremont House, 34 Molesey Road, Hersham, Surrey, KT12 4RQ
Telephone: 01932 255480
Website: www.securus-software.com