

Securus Offender Monitoring UK



Type of intervention



Online

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

(Potential)
Offenders

Tertiary Prevention

Young Adults (18-20 Years), Adults (21 Years +) | Male & Female | Online | Internet Related Only | English

Situations
/ Places

Internet/Online | English

Target population

Arrested and convicted Internet sex offenders in the UK. Securus is suitable for adolescent and adult offenders.

Delivery organisation (e.g. LFF UK, Prison Service of England and Wales)

Securus is available through the child protection charity, The Lucy Faithfull Foundation, UK. Various police forces within the UK and USA are also using the software.

Mode and context of delivery

Securus is e-Safety software, which examines personal home computers for specific inappropriate words and phrases and images, using a library which enables the recognition of such items. Results are monitored remotely by risk-management staff.

Level/Nature of staff expertise required (e.g. professional background)

Monitoring staff are police or ex-police officers, with a child protection background. Computer proficiency is essential.

Intensity/extent of engagement with target group(s)

A minimum of 12 months; the maximum is indefinite.

Description of intervention

The application of Securus monitoring software represents an attempt to enable arrested or convicted internet sex offenders to have full access to communications technologies, thereby potentially enhancing their attempts to achieve personal goals of agency, education, employment and intimacy which might prove more difficult with only restricted access to the Internet. It provides a degree of monitoring that removes the perception of anonymity and gives the offender a sense of responsibility and accountability for his/her own actions.

Securus is an e-Safety software package, which includes a remote computer monitoring tool. It was developed originally to protect children in schools from accessing prohibited websites and to curb the use of communications technologies for the purposes of bullying and/or sexual grooming.

The software has two key components: a physical, secure server appliance and client software that is installed on all PCs, laptops or remote devices, in the home of the offender, that are to be monitored. The server provides the central monitoring and control database and receives data from the client software. The client software monitors the user's PC 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 (Microsoft Office programmes, CD-ROMs, USB memory sticks etc.) Any text appearing on the screen is scanned for prohibited words and phrases, held on customizable 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 PC screen at the time of the event and records it, together with the user name, PC name, date/time and other important evidential information, all of which is then transmitted to the secure server. The software also alerts monitors 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 potential pornographic images. Those who manage these 'violations' can then log in to the server from a PC with Internet access, regardless of their location. All servers are physically tamper-proof and cannot be edited, altered or deleted, even during transmission of data.

Following an initial 6-month pilot project conducted by Surrey Police and the Lucy Faithfull Foundation, participants reported increased perception of being included and engaged in the risk-management process, allowing them to demonstrate to others both cooperation and positive online behaviour. These participants (offenders) preferred remote monitoring to additional home visits by the police for the purpose of monitoring computer use.

The use of Securus monitoring software helps offenders to stay safe online and relieves family members of any perceived responsibility for monitoring the offender's computer use.

Evaluation

Not yet completed.

References

Elliot, Ian A., Findlater, Donald and Hughes, Teresa (2010) *Practice Report: a review of e-Safety remote computer monitoring for UK sex offenders*, Journal of Sexual Aggression, 16: 2, 237-248.

Elliot, Ian A. and Findlater, Donald (2010) *A Review of a 'Managed Service' for the home computer use of Registered Sex Offenders*, The Lucy Faithfull Foundation, 'Securus' and Hampshire Constabulary.

Vess, J. (2008) *Sex offender risk assessment: Consideration of human rights in community protection legislation*. Legal and Criminological Psychology, 13, 245-256.

Ward, T., Gannon, T.A. and Birgden, A. (2007). *Human rights and the treatment of sex offenders*. Sexual Abuse: A Journal of Research and Treatment, 19, 195-216.

Contact details

The Lucy Faithfull Foundation

Telephone: 01372 847 160

Email: Wolvercote@lucyfaithfull.org.uk