University and College Union
Undeb Prifysgol a Choleg

Member briefing: ESafe information technology monitoring software

We are increasingly aware of instances where colleges are implementing the use of a new IT monitoring software, ESafe. We are mindful that this could lead to members' finding themselves in some difficulties. Therefore, staff should be careful when using college networks and only conduct personal searches, social media use and personal communications from their home networks. It is advisable for you to familiarise yourself with your institution's IT, ESafe and Social Media policies.

Below is an overview of the software, taken from ESafe's marketing info:

'ESafe software is a web based monitoring tool that currently monitors the digital activity of users in schools and colleges across the UK. ESafe uses a TripleLock system that combines a dynamic threat library, expert human behaviour analysis, and intelligent detection technology which provides early warnings of risks to the wellbeing and safety of those who are accessing the college's network.

The software identifies terms and phrases associated with risk categories such as; mental health, violence, drugs, extremism, bullying and pornography. ESafe's threat library is automatically updated with new markers of risk based on emerging behaviour and vocabulary trends, ensuring the safety, welfare and wellbeing of learners.

User activity is captured when a marker of suspected inappropriate activity or behaviour, which may impact the safety, welfare or wellbeing of an individual, is detected.

ESafe will:

- Detect from moving images
- Detect from static images, viewed or shared by users without accompanying text
- Monitor users when they aren't connected to the server
- Monitor users inside and outside of education hours in term time and holidays too.
- Transcend language and cultural barriers

ESafe software will monitor all data that is used on the college network, from running a search, emails and any external hardware used such as pen-drives and external hard drives. The software looks for certain phrases and words that might indicate a problem as far as safeguarding is concerned.

When a potential incident is detected, it is captured by our team of behaviour analysts, examined to assess whether it is a genuine safeguarding incident that needs further investigation. ESafe does not record the name of the user. User login IDs are assigned by the establishment and it is recommended that these cannot be linked to the names of the individuals being monitored, to ensure their anonymity is preserved. It is the responsibility of the establishment to ensure that all documentation that links user Login IDs to individuals is held securely and treated confidentially.

The following data is captured when a potential incident is identified:

- The User login ID
- The date and time
- The ID of the device that the User was logged into at the point the incident occurred (and serial numbers of various components within the device)
- A screenshot of the user’s screen at the moment the incident occurred

When incidents are determined to be genuine risks, ESafe will inform the establishment, providing a detailed incident report for them to investigate and determine the best course of action.'