GDPR

The protection of personal data is governed primarily by the General Data Protection Regulation. It affects the way organisations collect and store data, making it transparent and consistent.

eSafe is fully compliant.

eSafe has always had the greatest of respect for the data we routinely use in the course of our important monitoring work, and we are focused on achieving the highest of standards when it comes to the privacy and security of personal data that we process on the Customer's behalf.

The service will only capture user activity where a marker of suspected inappropriate activity or behaviour, which may impact the welfare and wellbeing of an individual, is detected. The service does not record all user activity nor capture details of apparently benign activity.

Personal data is only processed when necessary to provide the service , which is designed to detect the early warning signs of safeguarding risk as defined by the Department for Education, and as laid out in a formal Monitoring Services Agreement.

When monitoring the establishment's digital environment, eSafe will inform the establishment of safeguarding risk and criminal behaviour, to facilitate further investigation and intervention.

The service has been designed to minimise the amount of personal data recorded.

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

- **The service does not record all user activity nor capture details of apparently benign activity.**
- **Data is only recorded when a marker of behaviour affecting the wellbeing and welfare of an individual, or illegal activity, is detected.**
- **Most incidents captured for contextual review are anonymised with the use of user login IDs.**

When a potential incident is detected, we capture it so our team of behaviour analysts can examine it 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.

eSafe
REAL INTELLIGENCE
REAL PROTECTION

eSafe data is safe and secure at all times.

- All recorded data is held on dedicated servers located in an ISO 27001 accredited data centre.
- The data centre is based in the UK and only accessible by authorised eSafe employees, who are based in the UK. Data will never be exported outside the UK.
- No permission is ever granted to anyone outside of the UK to access any of the data hosted on eSafe servers.
- All eSafe staff are vetted by UK Police to NPPV-level 3, and include Security Cleared (SC) and Counter Terrorism Clearance (CTC) personnel.
- All eSafe behaviour analysts operate from a UK based, physically secure, ISO 27001 accredited laboratory.
- A wide range of security measures are in place to keep the personal data secure and enable it to be processed in compliance with the obligations imposed by Data Protection Legislation (under the DPA, obligations equivalent to those imposed on the Customer by the seventh principle of the DPA; under GDPR, the obligations imposed on the Service Provider by article 32 of the GDPR).

eSafe provides a similar service to various UK police forces and our data protection procedures, data security and physical security are routinely reviewed by the police to ensure our stringent standards are being upheld.

eSafe
REAL INTELLIGENCE
REAL PROTECTION

esafeglobal.com

eSafe Global, New Court, Regents Place, Regent Road, Salford, M5 4HB