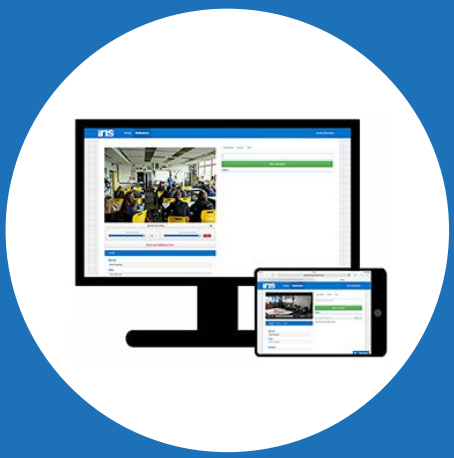
Security and data protection

Overview:



IRIS Connect is a sensitive professional development product. Not a surveillance system. We have thought very carefully about our responsibilities under the law, developing our system in line with the relevant legal frameworks. Protecting the rights and privacy of our clients is at the heart of our approach.

All data is:

- Secured in transit using SSL encryption
- Securely stored at rest within industry leading data storage (see below)
- Managed by a web platform designed to meet and, wherever possible, exceed our security obligations.
- Protected with industry-leading security provisions to negate brute force attacks and other potential online threats.
- Our security systems are regularly updated and reviewed by our in-house team of engineers working with the advice of industry leading consultants and are subjected to regular 3rd party penetration testing. Our staff are restricted from accessing client data by multiple levels of technical and procedural security.

End User Licensing:

Each IRIS Connect client nominates an Organisation Administrator who is responsible for agreeing to and enforcing the IRIS Connect End User Licence Agreement (EULA) when they first sign into the system. The terms of the EULA make the use of the system conditional on appropriate local agreements to ensure that all relevant parties are informed about the use of the system and have provided appropriate permissions for the capture and sharing of video. The EULA also stipulates that the system is used within a supportive developmental framework and that end users are aware of their obligations in responsible data management and sharing. This agreement also gives individual users the right to delete videos and ensures that individual videos will not be recorded or shared with any other IRIS Connect user without their explicit permission.

System Privacy:

The IRIS Connect system is based on individual user accounts and permissioning. This means that the observed user has to agree to a recording taking place before the system allows another user to connect to the camera. The same protections exist once a video has been encrypted and uploaded. This means users are only able to see data that has been explicitly shared with to them. By default users are limited to sharing videos with other users at their organization, although collaboration with other organizations can be enabled at the request of the clients Organization Administrator.

Users have complete control over who has access to their data by deciding to share observations either with individual users or into a group library. A fundamental principle of the system is that users will never “lose sight or control” of their video. They will always be able to see the video and any associated data. Users retain the right to delete a video or remove sharing privileges at any time.

Data Storage:

We store all data within a world-class environment trusted by numerous government and public sector organisations to store highly sensitive data. The environment utilises state-of-the art network security, electronic surveillance, physical security and multi-factor access control systems along to protect client data. The data centres are staffed 24x7 by trained security teams. This environment has qualified for the following assurance programs:

ISO 27001 (widely-adopted global security standard)
ISO 9001 (global standard for managing the quality of products and services)
G-Cloud (UK Government security standard)
FERPA (U.S. Department of Education)
FIPS 140-2 (US government security standard)
DIACAP and FISMA (US Federal Information Security Management)
DoD CSM Levels 1-2, 3-5 (US Department of Defence)
IRAP (Australia)
MTCS Tier 3 Certification (Singapore security management Standard)
PCI DSS Level 1 (Payment Card Industry Data Security Standard)
SOC 1/ ISAE 3402 (Service Organization Controls reports)
SOC 2 (Service Organization Controls reports)
SOC 3 (Service Organization Controls reports)
CJIS (US Criminal Justice Information Services)
CSA (Cloud Security Alliance)
HIPAA (Storage of protected health information)
FedRAMP (SM) (Federal Risk and Authorization

Data Protection and Retention:

In line with our role stated in the EULA we act as data-processors and our clients remain data-owners. In compliance with The Data Protection Act 1998 we are registered with the Information Commissioners Office in order to play this role. Unlike other online environments we do not, and will never ask for ownership of a clients data at any point.

We respect geographical regulations for data protection, such as the EU Data Protection Directive and as such ensure that we securely process and store all client data within their geographical region.

Customer Data (Financial):

Customer data will be retained in line with local legal frameworks

Customer Data (non-Financial):

IRIS Connect policy is for a maximum period of 2 years following termination of licence, although some data will be deleted prior to this based on the request of users. Our secure data centre employs industry-standard procedures on the decommissioning of it's storage devices at the end of their useful life.

There are certain occasions when information needs to be preserved beyond this limit; such as in the following circumstances:

- Legal proceedings or a regulatory or similar investigation or obligation to produce information are known to be likely, threatened or actual.
- A crime is suspected or detected.
- Information is relevant to a company in liquidation or receivership, where a debt is due to IRIS Connect.
- In the case of possible or actual legal proceedings, investigations or crimes occurring, the type of information that needs to be retained relates to any that will help or harm IRIS Connect or the other side's case or liability or amount involved.

Contact Us

w: www.irisconnect.co.uk **e:** info@irisconnect.co.uk **t:** 08453 038 578 **twitter:** @iris_connect