Security and Privacy Policy for theTeacherCloud Limited

This security and privacy policy is for users of the Evidence for Learning software and service, (http://www.evidenceforlearning.net), which is owned and operated by theTeacherCloud Ltd. In this document, 'We' means theTeacherCloud Ltd.

The Evidence for Learning Software and Service

The Evidence for Learning software and service allows organisations to collect, record, store, analyse and share (learning) data about their learners and other stakeholders. The service allows the organisation and its staff to share data with the parents and other stakeholders connected with the learners.

Security

Evidence for Learning stores the organisation's data on the device and in the Cloud.

On the device:

Only activated and licenced devices have access to data.

Photos and videos collected using the App are not automatically stored in the device camera roll or photo stream (outside of the app).

The app has passcode protection and your iOS device itself can be passcode enabled too which helps prevent unauthorised access.

Each of your devices is given a unique DeviceID and DeviceKey (like a username and password) granting permissions to access your (and ONLY your) data in the Cloud.

With a Cloud Subscription, the App can be remotely deactivated by theTeacherCloud should a device be lost or stolen. Passwords can be remotely reset.

Cloud infrastructure:

Our Cloud service is hosted on Amazon Web Services infrastructure (AWS) within the EU in highly secure, access-controlled data centers operated by AWS. (https://aws.amazon.com/security/)

Our services are configured as autoscaling, load-balanced, resilient environments, each configured across multiple geographically distributed availability zones. This ensures high levels of uptime and performance.

We have configured our environments to use VPC networks with robust security groups controlling access.

Our cloud infrastructure hard disks are encrypted, all data is encrypted at rest.

We use SSL/TLS 1.2 security at the network level to ensure all data is encrypted in transit.

Our User Manager tool forces a strong Password Policy containing a mix of uppercase, lowercase, numeric and special characters.

User passwords are salted and hashed using SHA512 encryption.

Our User Manager supports two-factor authentication (2FA).

Your Cloud Administrator has a password to maintain your system data stored in the Cloud.

Cloud data is protected with class-level and object-level Access Control Lists (ACLs).

We routinely conduct 3rd party security audits to verify the security and integrity of our systems and internal controls.

We have an internal data access policy that restricts access to personally identifiable information to a limited number of employees with a specific business need (such as for technical support).

No customer information is stored on individual employee computers.

We routinely monitor our systems for security breaches and attempts at inappropriate access.

Privacy Policy and Data Protection

In summary:

During normal use of the App, evidence photos, videos and data are transmitted from the app to our secure data centres.

All data transfer between a user's device and our data centres in the cloud is encrypted and happens securely via https using SSL.

The data stored in our data centres is used for no other purpose than to provide the services available in the App.

DBS/CRB-checked theTeacherCloud staff may access your data only to assist with support queries or maintenance.

All staff using the App should be subject to their organisation's policy on "Acceptable use of Electronic Communications".

Learners featured on evidence photos and videos should be subject to the organisation's standard "Parental Permission for Photos" policy where appropriate.

We are registered with the UK Information Commissioner's Office (www.ico.org.uk) and with the Data Protection Act 2008, registration Number Z3346221.

Under the terms of the Data Protection Act 1988, 2003, 2012 and the General Data Protection Regulations (GDPR) that came into effect in May 2018:

The organisation using the software and service is the Data Controller theTeacherCloud Ltd and its service providers are Data Processors.

It is the organisation's responsibility as Data Controller to be registered under the Data Protection Act and other relevant legislation and regulations.

Post-Brexit Update

We are monitoring developments very closely and will be adapting in accordance with any emerging legislation and guidance between now and 31 December 2020. In the meantime, during the Brexit transition period we will continue to comply with GDPR and the Data Protection Act 2018. Here's a link to the ICO quick guidance on GDPR post-Brexit and during the transition period:

https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqs-v2_3.pdf

What data do we collect?

For each organisation we collect and store:
-The name and address of the organisation.
-The name, email address and telephone number of staff and individuals at the organisation who pays for and/or use our service.

We store this information in order to administer, support and charge for the software and service.

You (the organisation) may additionally collect and store some or all of the following data on our service:

- The names and email addresses of the organisation's staff.
- The names, dates of birth, gender, email addresses of their learners and other data relevant to the learning needs and profile of your learners.

- The names and email addresses of the parents and related or relevant stakeholders of your learners.
- The contents of a Learner Profile:
    - Observations and assessments related to a learner's development, performance and progress.
    - Notes, photographs and videos of the learners and evidence related to their learning.

You (the organisation) have the freedom to choose which of the above data you store, and are able to delete it. You (the organisation) also choose who has access to the data.

In providing the software and service, we may from time to time send emails to staff and other stakeholders (such as parents) in order to confirm email addresses, reset passwords and may notify your users of events relating to the organisation's use of the software and service (such as when a new observation is added about a learner.)

We collect the following information from visitors to our sites:

- IP addresses
- Information about their web browser, device or computer
- Which pages people view

We use this information to monitor the security of our service, to help us improve the service and to improve the way we market the service (e.g. what search terms were used to discover our site).

We collect the following information from users of our tablet and phone applications:

- The make and model of the device
- The version of the operating system
- Details of any crashes that occur in the application
- Which screens people view in the application, although not the specific content of those screens

We use this information to help us improve the service (e.g., troubleshoot crashes)

We collect the following information about people who contact us by email or through our support ticket system:

- The person's email address, telephone number (if provided) and the contents of the email

We use this information to respond to questions or problems raised by our users.

When customers pay for our services, we may pass them to a Payment Service Provider (PSP), currently PayPal, which will collect the appropriate credit card and address verification details. We do not hold any credit card information ourselves.

How do we collect the data?

Data is typically entered by you and/or staff at your organisation directly into our software (either via the mobile application or web console). You (the organisation) may permit learners and other stakeholders (e.g. parents of learners) to add data to the service.

We may store cookies on users' computers and devices in order to verify that the user is logged in and to store their preferences. The cookies themselves do not contain any identifiable information about the user or the information they are looking at.

Information about the computers and devices that visit our site and access our software may be collected by Google Analytics and MixPanel, however NO information that is stored by you (the organisation) on our system is sent to Google or MixPanel. To clarify, Google and MixPanel are NOT able to view or access any data about your staff, learners or other stakeholders (e.g. parents of learners). You can read the privacy policy for Google and MixPanel here: https://support.google.com/analytics/answer/6004245?hl=en; https://mixpanel.com/privacy/

Who owns the data?

You (the organisation using the software and service) are the Data Controller.

theTeacherCloud Ltd and its service providers are Data Processors acting on behalf of the organisation (which is the customer of theTeacherCloud Ltd).

The only exception being that theTeacherCloud Ltd is a Data Controller for our own customer account information (e.g. for billing, administrative and support data and purposes)

Who do we share data with?

We do not share customer data, except as explicitly requested by you (the organisation).

You (the organisation) can provide access to data to your staff, learners and other stakeholders (such as the parents of learners).

The organisation and its staff can view, download or print some or all of the data and share it with other staff, parents, government agencies and any other stakeholders at their discretion.

theTeacherCloud Ltd, ONLY accesses and processes the data stored by you (the organisation) in order to provide, troubleshoot or improve the software and service.

To clarify, data collected and stored by you (the organisation) is not used for commercial purposes. We do not pass on any personal data or metadata for any commercial purpose and we will NOT sell or rent any information to any third party for any reason.

Can I (we) have my (our organisation's) data corrected or deleted?

Yes, you (the organisation) can correct or delete your data that is stored within the software by us, without the need to contact or involve us directly.

You (the organisation) can request that we correct the information we store about them. You can also contact us and we will correct or delete it on their behalf.

Data will be removed within 30 days of receiving request. At the end of a contract, leaving customer data is made inaccessible within 7 days and deleted

from the cloud after 90 days. The deletion of data will then be fully completed within 30 days. This gives customers time after contract end to retrieve their data. Once we have completed the deletion process we will notify you in writing to confirm.

What are your (the organisation's) responsibilities?

When you subscribe to and/or use our software and services, you agree to our terms and conditions.

You (the organisation that uses our software and service) have overall responsibility for complying with the Data Protection Act requirements (or the equivalent in other countries). It is your (the organisation's) responsibility as Data Controller to be registered under the Data Protection Act.

All staff using the App should be subject to your organisation's policy on "Acceptable use of Electronic Communications".

Learners featured on evidence photos and videos should be subject to the organisation's standard "Parental Permission for Photos" policy where appropriate.

It is important that you (the organisation) has taken care to:

- Think about what information it is appropriate to share with whom
- Ensure you have permission from parents or carers (where appropriate) for the data you wish to store about them and the way that you wish to use that data.
- Train your staff about sensible security and confidentiality precautions:
    - Taking care of passwords
    - Taking care not to install software on devices and computers that may compromise security.
    - Taking care not to access material from inappropriate places where it can't be kept appropriately confidential.
    - Prevent access to the software and service for stakeholders (e.g. parents) where the learner has been made inactive or has been deleted.

- Give stakeholders such as parents instructions for keeping the data protected.

Additional information...

https://aws.amazon.com/security/

https://aws.amazon.com/privacy/

https://aws.amazon.com/compliance/eu-data-protection/

For further information, please contact us at info@theteachercloud.net or dataprotection@theteachercloud.net