Youhere.org: Privacy Statement

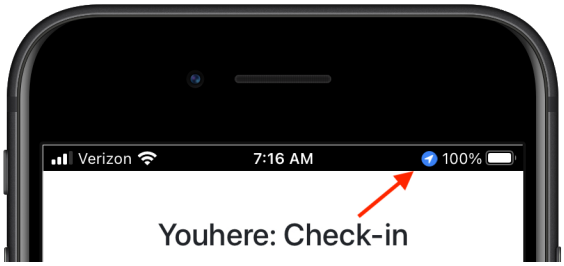
Privacy is a big issue at Youhere.org, as we deal with people and their location when they check-in. We know this. For a summary of our outlook on privacy, please see our privacy policy posted at Youhere.org. Below is some more (candid) information in this regard.

Participant Privacy

You're most likely worried about the privacy of your check-in participants. These are the people you are asking to check-in using the app. Go ahead yourself, and pretend you're one of your own participants and tap through the app, all the way to the point where you actually check-in to your own event.

Now, reflect on the steps you went through in order to check-in. You *were* asked for your name when the app was first opened. But reflect further. Were you ever asked for:

- An email address? **No.**
- Phone number? **No.**
- Physical address? **No.**
- The name or address of your school or organization? **No.**
- Any other web credentials? **No.**
- Messaging ID? **No.**
- Class schedule? **No.**
- Age? **No.**
- Gender? **No.**
- Did you have to make an account and set a password anywhere? **No.**
- Was your name verified in any way? **No.**
- Can our app determine your phone's number: **No** (it's technically impossible)
- Does our app track a person in real-time: **No** (look for a small indicator in the top bar of your phone (both iPhone and Android do this). This is shown by your phone's internals when an app requests location information. It only shows for our app when a user taps "check me in.")



As you can tell, the answer to these data-critical questions is "no." (We ask for the name of each checking-in soan attendance roster for the group leader. Pseudonyms may be used for this.)

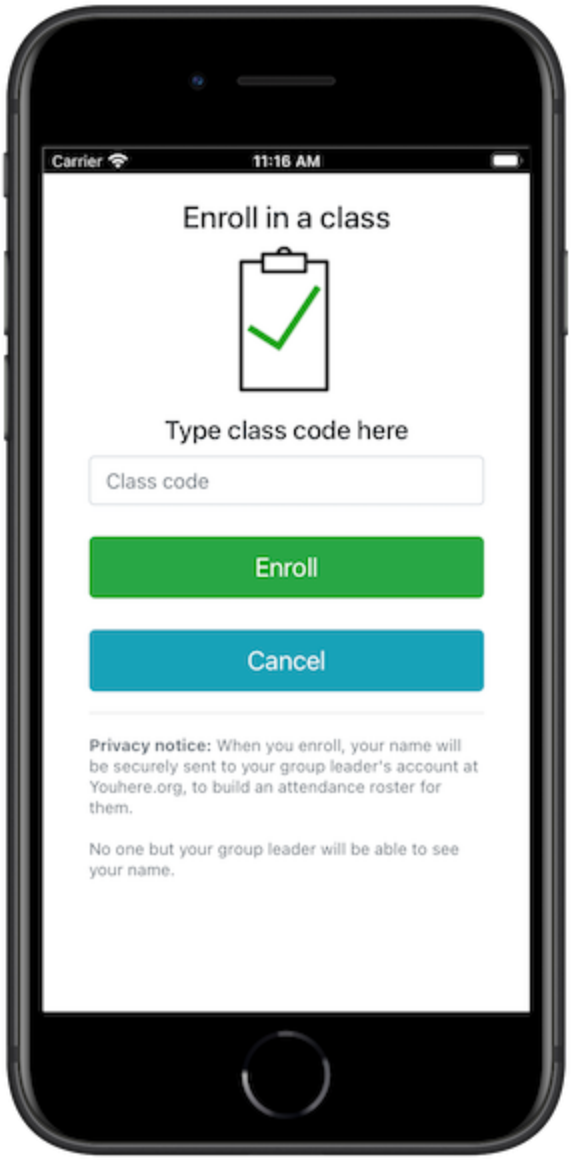
At a forensic level, about all we could do is *try* to do is manually (i.e. using Google, etc.) try to link student names with their check-in location to conclude for example (in the case of a student), that participant "Joe ,Person" goes to school XYZ. But 1) we have no interest in doing this (so we don't), and 2) this is semi-public information anyway (as anyone who sees Joe, Person at or around a school could find this out too, and/or the name might be in a school directory, on the (public) school website, or in a year-book or newspaper article, etc.).

Youhere was purposely designed to work with as little data as possible: a first and last name is the only personal information collected to build a roster only the group leader can see. Upon check-in, a location is pulled from the phone, to ensure one is within the needed location, and then it is discarded. Locations are never stored on our server.

As a reference, we ask one to reflect on just about any other online service in use (WhenIsGood, etc.). We think you'll find that Youhere likely collects *less data* than these other services. Think: What service works, by only requiring an unverified name?

The Youhere App

Our app moves flawlessly right through Apple's "do not track" privacy settings, which are part of iOS. We also never contact participants; but how would we since we don't have their contact information? Also very importantly, if a participant tries to check-in while outside of your needed location, their location is *not* stored. So if they're at the beach or in the mountains during an important meeting, no one will know that, and the app just responds with "sorry, you're out of range." Our App also has clear data privacy statements embedded right into the screens itself like this (see the "Privacy notice").



General Data Protection Regulation (or GDPR)

The European Union (EU) has a rather strict General Data Protection Regulation (or GDPR). We would like to address some of their core values in the table below (see **Article 5.1-2**) of the EU's GDPR:

GDPR Value	Youhere.org
Lawfulness, fairness and transparency — Processing must be lawful, fair, and transparent to the data subject.	Your name is used to build an attendance roster. Your location is used to verify that you're with the geofence your group leader needs, then discarded.
Purpose limitation — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.	(See above.)

Data minimization — You should collect and process only as much data as absolutely necessary for the purposes specified.	Nothing more than your name is collected. And your location is queried only when you tap the “Check me in” button. No other data is ever collected.
Accuracy — You must keep personal data accurate and up to date.	We don’t keep any personal data.
Storage limitation — You may only store personally identifying data for as long as necessary for the specified purpose.	We store attendance rosters as long as your group leader wants. When they choose to delete it, it will be gone.
Integrity and confidentiality — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).	All communication between the check-in app and our server is encrypted with https.
Accountability — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.	We are happy to reasonably demonstrate our commitment to GDPR standards at any time.

CIPA Compliance

CIPA (Child Internet Protection Action) is another safety metric we have studied. The points it focuses on are in the left column. How Youhere deals with a point is in the right column.

CIPA Point	Youhere.org
Access by minors to inappropriate matter on the Internet.	The App does not contain, point to, or include any inappropriate contents. It does not display any graphics, text or advertisements at all. It only displays buttons on the user interface, and short text-based information about check-in results.
The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;	Not part of Youhere.org. Minors or otherwise “participants” are not contacted by Youhere.
Unauthorized access, including so-called “hacking,” and other unlawful activities by minors online	Security is a constant concern and has ongoing and proprietary efforts underway.
Unauthorized disclosure, use, and dissemination of personal information regarding minors.	We do not collect any personal information from our users.

Measures restricting minors' access to materials harmful to them.	Youhere is appropriate for all audiences.

We stand by all of the information in this document and in our online privacy policy. At Youhere, we have over 1 million problem-free check-ins and counting. Contact us with any concerns or clarifications. We would be happy to speak with you via Zoom or otherwise if needed. Your school or department may have a privacy/data storage agreement or document, which we'd be happy to fill out and conform with.