# Checkology Overview and Data Security FAQ

Revised: 10/01/2020

### What is Checkology?

Launched in 2016 Checkology is a browser-based platform designed for students in grades 6-12 to help them learn, understand and navigate the most complex information landscape in human history — one in which truth, evidence and facts compete for attention with falsehoods, conspiracy theories and misinformation.

Checkology is owned and operated by the News Literacy Project and developed and maintained by Actual Size.

### What schools and districts trust and use the Checkology?

Many school districts across the United States are using Checkology, including the New York City Department of Education, the Los Angeles Unified School District, Miami-Dade County Public Schools, the Hawaii Department of Education, and hundreds more.

## Browser/Bandwidth Requirements

### What browsers and versions are supported by the Checkology?

Checkology operates within the following web browsers, including the last two major releases of:

- Chrome
- Safari
- Internet Explorer
- Edge

Checkology is optimized for both desktop and mobile usage using Windows, Apple or Chromebook devices.

### What are the Minimum Bandwidth Requirements?

A minimum 2.5Mbps connection is recommended.

### Do we need to Unblock anything to access Checkology?

Checkology is accessible by URL via HTTP and HTTPS. In addition to the checkology.org domain, clients should whitelist newslit.org and **at least one** of the following video hosting platforms:

- YouTube (https://youtube.com)
- Vimeo (https://vimeo.com)
- Wistia (https://wistia.com)

Videos on YouTube are uploaded as unlisted with no tagging. Vimeo and Wistia videos are private. All videos are considered safe for grades 6-12.

# User Information

## What User Information is collected?

Collection and encrypted storage of personally identifiable information (PII) for students and teachers is kept to an absolute minimum for viable usage of the product.

Collected information includes:

- First Name
- Last Name
- Email Address (*not required for students)*
- School & District Name
- Teacher & Class Section (Roster Data)
- Grade Level
- Student ID (Optional when using Roster Data)

## How do Students/Staff Log In?

Schools and districts can select from a variety of login methods that best suit their needs including:

- Email or Username/Password
- Google SSO
- Clever
- Schoology SSO

We are currently developing other methods of log in including LDAP, SAML 2.0 and others. Please reach out to us with additional questions.

## How do Student Usernames work?

In instances where student work is visible to other users of the platform, or when users need a username to login, students are represented by a username composed of their first letter of their first name, last name and a random number (in case of username duplication).

- Ex. randerson8
- For students, visibility of student usernames is limited to their individual class.
- For teachers, visibility of student usernames is limited to their class list. These are classes they've created or have been assigned a co-teacher for.
- School Admins, District Admins, and System Admins cannot see student usernames.

### How are Passwords stored?

All user passwords are hashed and encrypted using the same encryption techniques used to store PII, before they are saved to the Checkology database.

## Technical Information

### How are Data Transfers made?

PII is transferred from the client to the server with industry-standard SSL encryption, by way of a secure HTTPS connection.

If desired, clients may opt to pre-enroll their entire roster. This is a manual process, and specifics surrounding the transfer can be discussed by both parties.

As an example, Checkology can provide an SSH-accessible SFTP server and a public PGP key, with which the client can encrypt their roster (encryption at rest) and transfer it to Checkology (encryption in transit). Other tools, like established secure end-to-end encrypted transfer services, can be provided.

### How is Data Encrypted?

All PII is encrypted with OpenSSL to provide a minimum of AES-256 encryption. All encrypted values are signed using a message authentication code (MAC) so that their underlying value cannot be modified once encrypted.

Encrypted PII is only decryptable by the teacher(s) leading a student's section/class. Access to decryption keys are limited on Checkology's servers to the Checkology app itself and a root user (whose login is limited to SSH from identified administrators and is logged).

In addition to the application encryption, all system storage is encrypted by Amazon Web Services (AWS) at rest using a combination of industry-standard hardware and software encryption techniques.

### How is Checkology Hosted?

Checkology and related products are currently hosted on AWS EC2 instances. For general Amazon Web Services Security & Compliance documentation, please see their Whitepaper.

As an AWS customer, we inherit all the best practices of AWS policies, architecture, and operational processes built to satisfy the requirements of AWS's most security-sensitive customers. While AWS manages security *of* the cloud, we are responsible for security *in* the cloud.

### What types of Firewall or other Security measures are in place?

Checkology uses industry-standard AWS Security groups to firewall the application.

Incoming and outgoing web traffic is allowed for all IPs on HTTP and HTTPS. SSH connection to the server is limited by whitelist to preset list of computers.

### How does logging work on Checkology?

The system stores information needed to operationally debug and monitor the system for transaction failures and debugging. Logging actions taken within the system detail which user executes work; however, due to network configuration and layering the specific IP that the user was executing the work from is not accurate and as a result we do not retain it.

All logging (both in database and on disk) is securely maintained and only those who've been specifically granted access can access this information. Logging can be preserved for any desired Service Level Agreement (SLA).

### Does Checkology have a Disaster Recovery Plan?

AWS Data Centers are designed with carefully selected sites, redundancy, high availability, and ever-expanding capacity.

Within the Checkology system, we make automated backups and daily snapshots of the user database and keep each for at least 9 days.

## For More Information

### Who do we contact with questions about anything Checkology related?

We want to help you make the most of your Checkology experience. If you need any assistance with data transfers, usernames and passwords, or just want to tell us how we can improve please reach out to us at checkologyinfo@newslit.org.