SECURITY FACTSHEET

Contents

SECURITY FACTSHEET

Security Factsheet

Data Protection

Schoop is registered with the Data Protection Act (registration number: Z3641715) and school data is not shared with any other organisation. Only schools can access their own data.

Data Access

The Schoop web communications, web services, push notification servers and data are accessed over HTTPS with SSL (secure socket layer). This is a certified secure connection meaning all updates and communications including login is encrypted to the same standards as you would an online bank.

Please see this information about our Extended Validation SSL certification:

https://www.digicert.com/ev-ssl-certification.htm

No other organisation has access to your data. Authorised users can access their own data for the purposes of managing alerts, news, events and forms.

Data encryption

Schoop communications are one way, **non-sensitive**, and are meant to inform a wide audience of subscribers. Any personally identifiable information collected via forms or surveys is encrypted in our database and can only be decrypted by the Schoop software.

Location of Data and Servers

The data is held within a database on Windows Azure Cloud Services which are geo-redundant at sites which are SAS 70 type 2 certified.

See the Windows Azure Trust Centre.

 Last updated: 12/01/2015

SECURITY FACTSHEET

System Security

- Read the Windows Azure Trust Centre documentation for system security
- No data is stored on site. Data is only accessible to authorised data administrators.
- Data protection with 247/365 managed daily and incremental backup solutions

Operational Security - Infrastructure

- ISO17799-based policies and procedures, regularly reviewed as part of our SAS70 Type II audit process
- All employees trained on documented information security and privacy procedures
- Access to confidential information restricted to authorised personnel only, according to documented processes
- Systems access logged and tracked for auditing purposes
- Secure document-destruction policies for all sensitive information
- Fully documented change-management procedures
- Independently audited disaster recovery and business continuity plans in place for headquarters and support services

Operational Security - Application Environment

- Best practises used in strength checking of initial passwords
- All passwords are encrypted while in storage and are never sent in plain text format. Password reset system with fail safe notifications to users
- Secure media handling and destruction procedures for all customer data
- Email addresses are also encrypted

Physical Security

Please read the documentation in the Windows Azure Trust Centre