Online Scout Manager GDPR and Security Policy

Security of your data is our first priority and this page outlines some of our operating procedures and security practices.

The following information is correct as of 10th May 2018.

Definitions

We, our, us – Oneline Youth Manager Ltd

You, your, user – a young person logging on via the Leaders login page

Support Team – our employees or contractors who have access to provide support to you

Confidentiality

We place strict access controls over data and are committed to ensuring that nobody has access to your data that shouldn't.

If you contact our support team, you will grant them temporary access to your sections so they can provide support to you. Members of our support team are vetted and have strict rules and controls about what they can do with their access, and their usage is monitored. They cannot access your sections unless you contact support.

The operation of our systems requires that some of our employees and contractors have access to the systems that store and process your data. Our employees and contractors are prohibited from using this access to view your data unless absolutely required.

Our employees undergo periodic data, security and privacy training, and they are bound by Non-Disclosure Agreements.

Security Features

Logging

Usage of our system by users, the support team, employees and contractors is logged. We track every login, including the time, device details, IP address and a fingerprint of the device. This data is automatically purged after a period of time.

Access

We have a password policy requiring passwords to be at least 8 characters with two different types of characters, and the password is nt in the top 10,000 commonly used passwords. Passwords are stored using a non-reversible method.

We have compulsory second layer of authentication that requires all users to enter certain characters from an answer to a security question when they logon on a new device (if they aren't using Two Factor Authentication). The available security questions are obscure and are unlikely to be known by others (e.g. ''Mothers maiden name'' is not an option).

Users can opt to use Two Factor Authentication that proves them with a code that expires in 60 seconds.

Users are automatically logged out of the system after a period of inactivity.

Users who attempt to login with invalid credential too many times will be temporarily blocked from the system.

Users are encouraged to periodically review their access control list to ensure fellow users have the right access.

External Audits

We contract respected security firms to perform 'Penetration Testing' (sometimes known as 'ethical hacking') to ensure that data can only seen by the right people.

Infrastucture

Physical Locations

Our data is replicated in two separate data centres from separate providers on London to ensure that we can provide business continuity. We have off-site back-ups in a third location.

Data

We do not share personal data to third-parties with the exception of text messaging, email providers, and payment providers for the instances where users sends text messages, emails, and when payments are collected via the payment providers.

We are not responsible for the data that users add within the system, including its accuracy. This includes, but is not limited to, contents of external links, activities, emails, downloads and attachments.

Mobile System

Our mobile system stores data for offline use by users – sensitive personal data is encrypted on their device.

The system automatically removes data help on the device when the user no longer has access to the section. In the event of a device being lost, users can contact our support team to tell the device to remove its data when it is next used online.

Encryption

Our data is encrypted in transit and at rest.

Database backups are encrypted individually and off-site backups have full disk encryption too.

Our employees' computers have full-disk encryption (although your data is not stored on employees' devices).

Intrusion Detection System

We have systems that monitor the usage and automatically block users who appear to be malicious.

Firewalls and Software Patching

Firewalls are configured according to industry best practices and all unnecessary ports blocked.

We perform automated network vulnerability scanning and software patching.

Backups

System-wide backups are held off-site for a period of six months.

Legal Jurisdiction

We operate under the laws of England and Wales.

Payment Providers

Braintree

Users may pay for services using a credit or debit card. We use Braintree Payments to process the data – we do not store and cardholders data.

PayPal

Up to 2016, we used PayPal subscriptions for payments. Subscriptions cannot be modified by us (other than manually cancelling them).

GoCardless

Parents are able to make payments to their respective groups. Payments are handled by GoCardless, who are regulated by the Financial Conduct Authority. We do not receive bank details.

Data Subject Rights (GDPR)

Breach Notification

We will only notify our users of any breach of data via email with 72 hrs of identifying the breach.

Right to Access

Users are able to download information about members if required, and the support team can provide assistance if the downloads are not sufficient.

Right for Erasure

Users are able to delete all personal data with the exception of audit trails. Users can contact the support team for ‘Right for Erasure’ requests.

Data Portability

Users can download personal information in a spreadsheet format. It should be noted that this requirement is only applicable if you use ‘consent’ for your lawful processing mechanism. ‘Legitimate interests’ is likely to be more appropriate and therefore consent is not required, as the data provided bt parents is expected to be stored and processed for the purpose of running a Group/Unit and its associated events.

Privacy by Design

Our system is always designed with privacy as our top priority. Features are tested manually by our expert developments teams, automatically as part of the development & deploy process, and through external security audits.

Data Protection Officer

Ed Jellard is the Data Protection Officer. He can be contacted via the Contact Us page.

The Scout Association’s ‘Third Party Processor Checklist’

This section provides a generic response to the checklist The Scout Association has provided.

GDPR compliance

OSM is GDPR compliant – see above for details of the technical and organisational security measures.

Personal data search

OSM allows you to view members you have access to, subject to your permission levels.

Personal data deletion

OSM allows you to delete all personal data with the exception of the membership history (the audit trail of changes). There will be a deletion mode to allow you to delete this too.

Standard contract terms

Our legal team is creating a data processing agreement/contract that will include GDPR provisions.

Data processing records

We have a data processing document that is available upon request.

Breach notification process

We have a document breach notification process that includes notifying administrative users of OSM via email and the ICO.

Data portability

While the data is only a requirement for the ‘consent’ lawful processing mechanism, we do provide spreadsheet downloads of personal data.

Sun-processor change request process

We use industry-leading sub-processors and therefor do not have the ability to request changes.