Terms of Use & Security

HOPS

Reviewed 27/01/2021 - New text shown thus.

Data Protection & Security

All data we hold is secured to the full extent required by the Data Protection Act / GDPR. This includes, but is not limited to:

- Running a secure operating system (Debian Linux), with operating system and application security updates applied in a timely manner.
- Maintaining a firewall to prevent unwanted access to the server.
- Providing secure access to the website over HTTPS, to prevent snooping of data or man-in-the-middle attacks.
- A permissions system to prevent unauthorised access, modification and deletion of data through the website itself.
- Offsite backups to prevent loss of data through hardware failure or accidental damage.
- Hosting the server and backups in a secure third-party physical location.
- Limiting login to the server itself to the administrators of HOPS.
- HOPS is exempt from registration with the Information Commissioner's Office (ICO), however, we have elected to voluntarily register (ZA096228).
- Our track record: In the ten years we have been running HOPS, we have not had a single problem related to unauthorised access to data. In that time we have been trusted by over 100 orgaisations to store data for over 25000 users.
- When a user is archived from HOPS some data is retained indefinitely for recording purposes, ie, names on rosters. Other data, including contact information, etc, is removed after a suitable period. The period is currently two years, but is shortly to be reviewed.
- Users may request disclosure of all information held about them in HOPS. Requests of this nature should be addressed to the user's home organisation for data for which that organisation is the data controller and to HOPS for data for which HOPS is the data controller.
- HOPS will only change the point of contact at a railway (and hence the person from whom we will take instruction on the use or release of the railways data) following a reasonable corroboration of the validity of the request for the change, and reserves the right to refuse such requests if we suspect they are not legitmate.
- User account passwords are stored in the database in encrypted form, from which they cannot be decrypted. Passwords are not visible by the programming team nor anyone at any railway. For this reason passwords can never be revealed even to the user to whom they belong. If a password is forgotten it can only be reset to a new random password.
- Records are kept of all users' activity on the site.
- HOPS maintains the following response plan for a breach of data security:
    - Clients / Data Controllers will be advised as soon as possible.
    - Advice will be given to clients (potentially including advice to pass to their users) regarding how to protect themselves from the potential for their data to be used maliciously (ie phishing emails etc)
    - Investigation will take place within HOPS to determine the failure of systems or processes that led to the incident, and actions taken to prevent a reoccurrence.
    - If necessary, further updates will be given to clients.
    - HOPS will NOT advise users directly where the breach relates to data for which HOPS is not the Data Controller.
    - The UK ICO will be advised where appropriate / notifiable.
    - HOPS will not advise any non-UK authorities, that will be the responsibility of the data controller.

If you would like more information about HOPS please contact us.