Quick Start guide: registering administrators on the Platform

THIS GUIDE IS INTENDED FOR ADMINISTRATORS

Please note:

- Training is available for neutrals and the parties' representatives. Please contact Tony Guise to arrange – please email tonyguise@disputesefiling.com.

- A statement about data security is at the end of this Guide.

- At the end of each case all registered users (including neutrals) will receive an email containing a link to a short online survey. We ask that users complete this to assist with evaluating the performance of the Platform.

This is our quick guide to using the Platform:

Steps:		Action
1	Use your web browser to find the log in page	https://oneplatform.disputesefiling.com
2	Ensure your IT department completes some preliminary steps	Please ask your IT Department to: • set firewalls so as not to block our emails • check our emails are not treated as spam • ensure our emails are not sent to your junk email folder • whitelist the IP addresses 81.29.93.247 and 5.153.73.108 • ensure your computer is protected by an appropriate anti-virus program If you prefer contact our Support Desk on 0203 143 3333 and provide our IT support staff with your IT Department's contact details and we will do this for you.
3	The Administrator needs to register and be validated.	PLEASE NOTE THERE ARE VARIOUS ADMINISTRATOR ROLES ON THE PLATFORM. PLEASE ENSURE YOU REGISTER IN THE RELEVANT ROLE FOR YOUR ORGANISATION Those acting as Administrators must register on the Platform. The registration process prompts choice of role. Complete the required boxes ensuring you type email addresses accurately and we prefer you not to use a free email service e.g. Gmail. Corporate email addresses

		work most effectively e.g. tonyguise@disputesefiling.com The Platform Provider (DisputesEfiling.com Limited) has a Validation Desk which is required to complete validation within 48 hours.
4	Neutrals or other users should register and follow the instructions in the emails you will receive following registration	Once a neutral or other user has registered he or she cannot access the entire case unless validated by his or her Administrator. The Scheme Administrator will receive an email requesting that he or she validate an applicant by logging in to the Platform and going to Confirm Users where he or she will see flagged the name of the user(s) to validate. Then follow the on screen prompts to validate or refuse validation.
5	If already registered, log in by clicking the log in tab and enter your user name and password	Complete the required boxes
6	If the Administrator is acting as a neutral or other user and wishes to access his or her own cases or view cases worked on by any user registered to him or her as Administrator.	Log out as Administrator and log back in using the email address you registered for the other role. Click the tab marked “View Cases” across the top of the screen beneath the panoramic image.
7	Go to View Cases in order to choose a case to work on or review	Scroll down the list of case names and use the cursor to click on (and thereby open) the relevant case
You are good to go!		

There is support available via the Platform including Frequently Asked Questions (FAQs) and telephone support via the number on the support pages. Just click the link at the top right hand corner of every Platform page to reach the support pages.

DisputesEfiling.com Limited

Statement concerning data security

Valid as at: 13.12.18

The security and protection of our clients' data is our greatest priority.

For obvious reasons a detailed explanation of the security measures in place cannot be provided in order to protect the integrity of the data centre's security.

In summary the following are covered by our security technologies and controls:

- Data encryption
- Network encryption
- Security information and asset management
- Trained cloud security professionals
- Intrusion detection and prevention
- Vulnerability assessment

Within these fields of activity we strive to protect our users' data as described in more detail below.

The General Data Protection Regulation (GDPR)

Together with colleagues in our partner organisations we provide full compliance with the Data Protection Act, 2018 and the GDPR.

Our compliance actions are constantly evolving as we respond to developments in the regulatory environment and ever changing cyber threats.

It is important for users to recognise, accept and actively play their part in ensuring the data uploaded is as secure as we can make it by working together.

Password safety

We urge our clients not to use the same password in multiple contexts as this will reduce the security of the data. We also ask them not to email passwords.

Passwords should be strong in formation i.e. at least 7 characters comprising a mixture of upper case and lower case letters, symbols and numbers.

Access to the platform is via a two stage gateway involving user name and password.

Some information about our data centre

1 The centre's servers are regularly updated with security patches and fixes.

2 The Platform itself is written in terms that follow best practice for validating user input and protecting the database.

3 The servers sit behind firewalls and intrusion prevention systems which protect from internet based perimeter attacks.

4 The security of the Platform is under constant review in the light of reported hacks of well-known organisations.

5 No payment details are stored on the Platform.

6 Passwords are kept in an encrypted form on the database.

7 All data sent to and from the Platform including log on details are sent via SSL (encryption).

8 On site staffing 24 hours a day.

9 Multi-layered physical security including:

a) CCTV and recording

b) Data centres located in South East England enable site resilience for core services

c) All backup data is transmitted between the data centres' sites via a military grade (AES-256) encryption key. It is then stored in UK data centres with this encryption.

d) Power resilience using multiple connections to the National Grid

e) Redundant capacity components physically available on site.

f) The centres are equipped with on-site generators with UPS and battery systems for transparent fail-over.

g) Fire threat detection and suppression.

h) Water leak detection

i) Multiple up-links in place.

j) All components are fully fault-tolerant including the up-links, storage facilities, chillers, HVAC systems and servers.

We host at Tier 3 data centres which meet the following standards: ISO 27001, ISO 9001 and PCI DSS 3.0.

These measures enable the data centre to guarantee the availability of data from the hardware for 99.982% of operational time.

<u>Encryption</u>

Unlike other e-mail systems such as Outlook, any emails sent via our platform use 3DES encryption as a minimum together with additional encryption measures making web communications and their attachments secure.

END