

King's Ely: Libra ESVA: Understanding the inbound email scanning software: Control your own preferences of which emails reach your mailbox or are blocked

The School's virus scanning/protection for inbound emails is through a system called Libra ESVA. This system scans all incoming emails against known threats, viruses, ransomware, and content/key words associated with anti-radicalisation and other "dictionaries" such as words associated with adult content. In addition, it assesses each email for the probability of it being legitimate or spam/junk. All of this happens before the email comes into the school's email servers.

By default, each day, at 4am, a list of any such trapped emails is sent to each user, setting out the details of their own trapped emails (who from, title, etc) and a reason for the email being held up. An example of such a message is below.

E-mail Quarantine Report for: SimonDrew@kingsely.org

In the last 24 hours you received 1 e-mails that were quarantined, as listed below. All messages in the quarantine are automatically deleted 60 days after the date that they were received.

The list is ordered by Spam Score, with the messages considered least like spam at the top.

- Virus = mail with harmful content - can not be released
- Bad Content = mail with invalid content
- Infected = mail with script in content - can not be released
- Spam = mail is supposed to be unwanted
- Blacklisted = sender is listed on local blacklist

Received	From	To	Subject	Score	Reason	Preview	Actions
25/06/18 13:01	bb@xmr3.com	simondrew@kingsely.org	The World of Entertainment	5.21	Spam	[View]	[Release] [Rel. & Whitelist]

Apart from emails blocked because of a virus threat or malicious script embedded within (these are quarantined) or has content that matches keywords within certain "dictionaries" (these are sent to a special mailbox for a member of our DSO team to review), users can control what they do with suspected spam or previously Blacklisted emails. You can choose to Preview the email (in a safe way – it does not come into your mailbox), "Release" the email (release it this time into your mailbox) or if you know it to be legitimate, and you wish to allow emails from that source in future, you can "Release and Whitelist" the email, thus teaching Libra your personal preferences.

Once an external originating email reaches your inbox, you have a further a choice to mark it as spam or blacklist the sender (these options can be found at the very bottom left of an external originated email not manually released through Libra – see example below). It is normally best to try to unsubscribe to any marketing type emails before Blacklisting them (GDPR has helped in this regard).

This message has been checked by Libraesva ESG and is found to be clean.

[Click here to mark it as spam.](#)

[Click here to blacklist sender](#)

Each user can check their own White and Blacklists and configure other things like changing or adding times of the day Libra reports/lists are sent to you. You can do this by going to: <https://kingsely.esvacloud.com/>.

1. Upon enter Libra you will be prompted to enter your **@Kingsely.org** email address. Click **Continue** to proceed. Highlighted below in red.



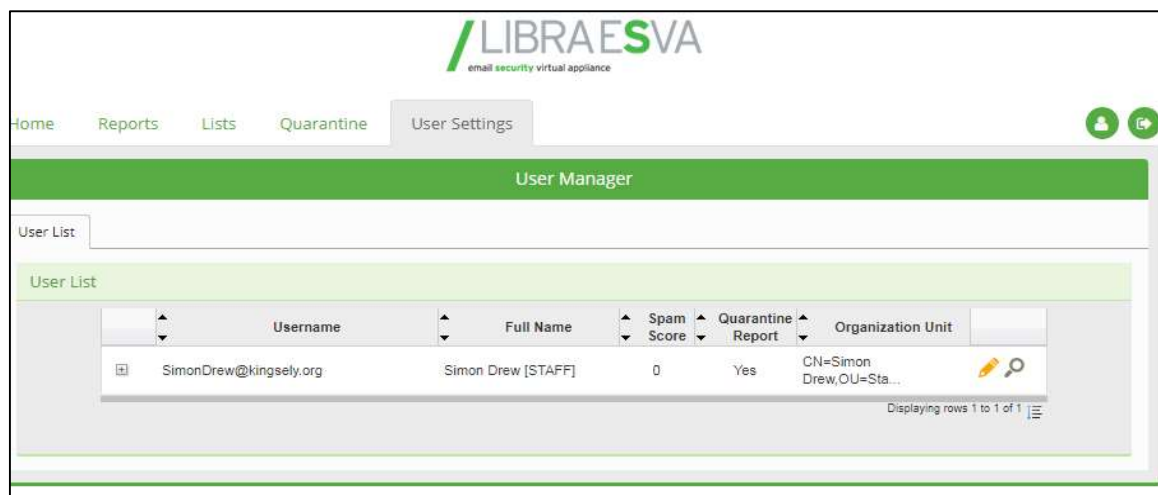
The screenshot shows the 'Email Security Login' page. At the top left is the 'LIBRAESVA EMAIL SECURITY' logo. Below it is a teal header with the text 'Email Security Login'. The main content area says 'Please enter your credentials to login.' followed by 'Username or Email' in bold. Below this is a white input field with a red border. Underneath the input field is a teal button labeled 'Continue'. At the bottom of the page, there is a teal horizontal line and the URL 'http://www.kingsely.org'.

2. You will now need to enter your password. Click the **Sign in** button to continue.



The screenshot shows the 'Email Security Login' page. At the top left is the 'LIBRAESVA EMAIL SECURITY' logo. Below it is a teal header with the text 'Email Security Login'. The main content area says 'Insert password for' followed by 'liamwagstaff@kingsely.org' in bold. Below this is a white input field with a red border. Underneath the input field is a teal button labeled 'Sign in'. Below the button is a link that says 'Forgot your Password?'. At the bottom of the page, there is a teal horizontal line and the URL 'http://www.kingsely.org'.

Once logged into Libra, you can manage your settings under the **USER SETTINGS** Tab (click the little pencil icon to edit any settings such as times of day to receive your Libra reports); view a list of emails that have been quarantined under the **QUARANTINE** Tab; and manage your own White (allowed) and Black (disallowed) lists under the **LISTS** tab. If you see an email address in your Blacklist that is a legitimate contact, you should delete that entry in the list so future emails are allowed through to you.



If at any time you are prompted to Login again. Please refer to steps 1 and 2 mentioned earlier in the guide.

Over time, with you teaching the system your preferences, you should see a reduction in spam email arriving in your inbox. Please be aware that any emails trapped and not released are deleted after 30 days (so would not be able to be retrieved via the **QUARANTINE** tab described above).

Should you encounter any issues in this process please raise a support request via the **ICT Support Ticket System**. This can be done by clicking the RM Support application located on the desktop of any school device.