EVOLVE Password Policy

Users access EVOLVE to plan and manage visits, record incidents and manage extra-curricular club and activity programmes. The system provides a range of features to ensure that access to the system, and specific parts of the system, are restricted to appropriate users:

Access Controls

There are 5 user levels in the basic permission hierarchy. Each level between Level 1 and Level 4 adds additional functionality or scope onto the previous level. In addition to the Levels 1, 2, 3 & 4, there are System Administrator Users that have access to the online control panel and can amend system settings (e.g. turn features on and off). A user can be a member of any one or more User Level.

Password Requirements

- ✓ All passwords should be sufficiently complex for unauthorised users to guess.
- ✓ EVOLVE passwords must be a minimum of 8 characters in length.
- ✓ EVOLVE passwords must contain at least one alpha and one numerical character.
- ✓ EVOLVE passwords cannot be re-used. Users will need to choose a new password each time they change, or are forced to change, their password.
- ✓ If the security of a password is in doubt, the password must be changed immediately.
- ✓ The chosen password cannot be the same as the username.

Password Recommendations

- ✓ Users should use common sense when choosing passwords and avoid basic/common words and names.
- ✓ Why not pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalisation? For example, the phrase “You have hit the nail on the head” can become “81YhHTn0tH!”.
- ✓ Users should not share passwords with anyone including colleagues, managers, IT staff members, etc. We will never ask for passwords when dealing with support requests.
- ✓ All users who should have access to EVOLVE should have their own user account.
- ✓ Users should avoid writing passwords down and avoid using the "Remember Password" feature of applications, especially if working on a shared computer.

Additional Security Features

The following additional security features can be configured.

Access Controls – These additional security settings allow you to control access to a range of EVOLVE features outside of the User Levels structure. For example, you might want to restrict access to a particular feature to a named user, or several named users, rather than any user of a particular User Level. Access Controls can be configured by System Administrator accounts.

Password Expiry Periods* – Setting a password expiry period will require all users to update their password according to the schedule specified by the EVOLVE System Administrator in the Data & Security Dashboard.

Password Reuse* – EVOLVE System Administrators can set the password re-use policy, e.g. how many previous passwords are remembered and disallowed for reuse, from with the Data & Security Dashboard.

Automatic Log-in Restrictions – EVOLVE will automatically disable a user account that has experienced multiple failed login attempts. EVOLVE system administrators can configure this setting from the Data & Security Dashboard.

Automatic IP Address Blocking – EVOLVE will automatically block requests from an IP address that is identified as making multiple failed login attempts within a short period of time.

Session Time-out periods* - EVOLVE will automatically log users out of the system after 20 minutes of inactivity. This period can be configured from with the Data & Security Dashboard.

Two-Factor Authentication* – Activating Two-Factor Authentication will alter the log-in process so that in addition to requiring a valid username and password, the user will be required to enter the 6-digit code that is sent to the email address that is registered with their user account each time they log on.

Email Single Sign-On (ESSO)* – This feature provides a convenient Single Sign-On (SSO) solution. When enabled, users can simply enter their username in the EVOLVE log in screen and then click the link in the email that is sent to the address registered with their EVOLVE account. No need for users to remember multiple passwords; they can access EVOLVE from their email inbox

*An online interface to configure these additional features will available in May 2018