Royal Conservatoire of Scotland

Password Policy

Document Revision History

Version No.	Version Date	Prepared By	Approved By	Summary
1.1	July 2014	Kelly Ward	Fraser Ross	RCS Password Policy
1.2	April 2017	Kelly Ward		Update to special characters allowed
1.3	August 2021	Kelly Gardiner	Fraser Ross	Password expiry date, MFA update, password guidance
1.4	January 2023	Kelly Gardiner	Allan Cameron	Update to password length and guidance

Password Policy

1. Introduction

Passwords are an important aspect of computer security; a poorly chosen password can compromise the security of the Conservatoire's entire network. As such, all Royal Conservatoire of Scotland employees and students who are issued with a user account are responsible for taking the appropriate steps, outlined below, to select and secure their passwords.
Where possible, the Conservatoire will implement Single-Sign On (SSO) technologies to allow a user to authenticate seamlessly.
All employee and student accounts require Multi-Factor Authentication (MFA) to be enabled on their account as an additional layer of security.

2. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change.

3. Scope

This policy applies to all employees, contractors, consultants, temporary and other members of staff at the Conservatoire who have, or are responsible for an account on any system that resides at Conservatoire facility. It also applies to all registered students.

4. Password Policy

Users must note that User ID and passwords assigned to them are for their own personal use, and must not be shared or disclosed to any third party.

Passwords will not expire, however if you suspect your password has been compromised you must change it immediately and report this to the IT Department.

When a password is changed, the owner must create a password that is different from the last 3 passwords

If an incorrect password is entered 6 consecutive times, the account will be locked out. If you have enrolled for our Self Service Password Change program, you can unlock your account using this service.

All passwords must contain no less than 15 characters, although longer passwords are recommended.

All passwords must contain characters from 3 of the following 4 categories

- English uppercase letters (A-Z)
- English lowercase letters (a-z)
- Numbers (0-9)
- Special characters e.g $!@

Please note that the following special characters are not allowed

" & \ £ '

Passwords should never be written down, stored on-line or sent in an email message

5. Password Guidelines

The password should not contain common usage words such as:

- Names of family, pets, friends or co-workers, etc
- The words "Royal Conservatoire of Scotland" or "RCS" or any derivation
- Birthdays and other personal information such as addresses or phone numbers
- Word or number patterns, like aabbccdd, 1234567, etc
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit

Passwords should not be the same as usernames

Do not use the same password for Conservatoire accounts as for non-Royal Conservatoire of Scotland accounts, e.g. personal email account.

Try to create a password that can be easily remembered. The National Cyber Security Centre advises to use 3 random words. Numbers and symbols should be added where needed. For example, 6yellowhousedogs54!

Be creative and use words memorable to you so that people can't guess your password. Remember that your social media accounts can also give away vital clues about yourself so avoid using words that are easy to guess.

Do not use any of the example passwords in this document.

If you suspect an account or password has been compromised then you should report this to IT Helpdesk immediately and change your password.