ICT Password Policy

ICT Password Policy

1 Statement of Policy

1.1 All staff and students of The Constellation Trust must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of IT's strategy to make sure only authorised people can access those resources and data.

1.2 All staff and students who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorised people.

1.3 The purpose of this policy is to make sure all the Trust resources and data receive adequate password protection and comply with General Data Protection Regulation (GDPR) May 2018. The policy covers all staff and students who are responsible for one or more account or have access to any resource that requires a password.

2 Password Creation

2.1 All passwords should be reasonably complex and difficult for unauthorised people to guess. Staff and students should choose passwords that are at least 8 characters long and contain a combination of upper and lower case letters, numbers and punctuation marks and other special characters. These requirements will be enforced with software when possible:

- Minimum password length – 8 characters
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Allow the password to be same as the previous 3 passwords
- Contain characters from three of the following four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example: !, $, #, %)

2.2 In addition to meeting these requirements, staff and students should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like: 'password', 'password1' and Pa$$w0rd' are equally bad from a security perspective.

2.3 A password should be unique, with meaning only to the member of staff or student who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended

method to choosing a strong password that is still easy to remember: pick a phrase, take its initials and replace some of those letters with

2.4 numbers and other characters and mix up the capitalisation. For example, the phrase ‘this may be one way to remember’ can become: ‘TmB0WTr!’.

2.5 Staff and students must choose unique passwords for all of their school/academy accounts, and may not use a password that they are already using for a personal account.

2.6 All passwords will require to be changed regularly, with the frequency varying based on the sensitivity of the account in question. This requirement will be enforced using software when possible.

2.7 If the security of a password is in doubt – for example, if it appears that an unauthorised person has logged in to the account – the password must be changed immediately.

2.8 Default passwords such as those created for new staff and students when they start or those that protect new systems when they are initially set up must be changed as quickly as possible.

3 Protecting Passwords

3.1 Staff and students must never share their passwords with anyone else in the school/academy including: co-workers, managers, administration assistants, IT staff members, friends, etc. Everyone who needs access to a system will be given their own unique password.

3.2 Staff and students should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All staff will receive training on how to recognise these attacks.

3.3 Staff and students must refrain from writing passwords down and keeping them at their workstation. See above for advice on creating memorable but secure passwords.

3.4 Staff and students may not use password managers or other tools to help store and remember passwords without IT’s permission.