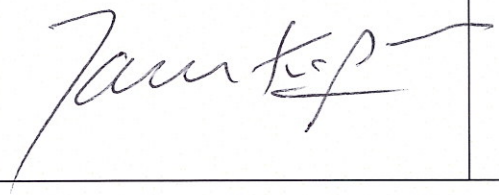
THE DEAN TRUST
Believe Achieve Succeed

IT PASSWORD POLICY
STAFF & STUDENTS

CENTRAL POLICY

Version and Date		Action/Notes
1.0	September 2016	Policy created by Group IT Manager,
2.0	November 2016	Reviewed and updated
3.0	April 2018	Reviewed to reference GDPR

Policy Reviewed:	April 2018
Policy Review Frequency:	Every 2 years
Next Review:	September 2020
Signature of CEO: 	**Signature of Chairman of Trustees:** 

Objective

The Trust is committed to ensuring that IT systems are secure and Trust data (as well as that of individual Schools) are only accessed by authorised users.

Policy

All Trust systems enforcing password restricted access must implement the following password rules where systems support them.

- All passwords must be of a minimum length of 8 characters
- Passwords must contain characters from at least three of the following four categories:
  - Lowercase letters a to z
  - Uppercase letters A to Z
  - Numbers 0 to 9
  - Special characters ! # $ % ‘ ( ) + ? @ [ ] ^ _ { } ~ -
- Passwords must not contain any characters that are not listed above, including space characters
- Passwords must not contain the user’s first name, surname or logon code and for students, also their student number
- Staff and student passwords will expire after 90 days by default or less depending on contractual requirements of some third parties
- The previous 8 passwords cannot be re-used

All exceptions to this policy e.g. for technical systems or if different levels of password security are required to meet contractor obligations, must be approved by the Group IT Manager.

Scope

This policy applies to all staff, students, data processors, partners, suppliers and contractors, in addition to any other authorised users. The policy applies to secure access to all the Trust's IT systems, which should where possible use the Trust's standard directories for authentication. Where this is not possible they should implement this policy within their own systems. As above, any exceptions for technical reasons must be documented and approved.

Implementation, guidance and good practice

Guidance and good practice on setting passwords for staff will be published on the IT Department Moodle page