TDAP052B
PASSWORD POLICY

Requisite: Dorcan Requirement				Responsible Committee: F&P	
Vers.	Approval Date	Committee	Head	Chair	Next Review Date
A	18/06/2018	*Finance and Premises*			October 2021
B	13/01/2022	*Finance and Premises*			January 2025

Rationale

This policy has been created to help enforce data protection recommendations across the Academy and to minimise the risk of data breaches in relation to all personal or sensitive data.

Purpose

The ICT Support Team will be responsible for ensuring that the Academy networks are safe and secure as is reasonably possible.

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission
- access to personal data is securely controlled in line with the federations personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure password policy is essential if the above is to be established and will apply to all ICT systems, including email. The ICT team will be responsible for ensuring that users conform to the policy on a day to day basis.

This policy applies to all employees and students.

Policy

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the ICT Support Team and will be reviewed, at least annually.
- All academy ICT systems will be protected by secure passwords that are regularly changed.
- The "master/administrator" passwords for the school/academy systems will be made available to selected members of the ICT Support Team and SLT.
- Passwords for new users will be allocated by the ICT Support Team. Replacement network/application passwords will be allocated by the ICT Support Team or authorised Academy personnel with access to specific tools. If allowed self-service password software can also be used by the end user. Authorised personnel are identified with the appendices.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

on details and must immediately report any suspicion or evidence of a breach of security to the Data Protection Officer.
- Users will change their passwords at regular intervals in accordance to guidelines outlined below.
- Requests for staff password changes will be recorded using the ICT Support Teams service desk system. If required, solutions will be put into place to allow dedicated staff to change pupils/students passwords.

Staff passwords

- All staff users will be provided with a username and password.
- The password should ideally be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
- The password should not include proper names or any other personal information about the user that might be known by others.
- The account should be "locked out" following six successive incorrect log-on attempts.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption). Passwords will not be left on public display, or written down in an unsecured location.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Should be changed at least every 90 days.
- Should not re-used for 6 months and be significantly different from previous passwords.

Student passwords

- All users will be provided with a username and password.
- Students will be taught the importance of password security.
- The complexity will be set with regards to the cognitive ability of the children.

Training/Awareness

Members of staff will be made aware of the school's password policy:
- at induction
- through the Academy's e-safety policy and password policy.
- through the Acceptable Use Agreement.

Students will be made aware of the school's password policy:
- in lessons when teaching the Digital Skills curriculum
- through the Acceptable Use Agreement

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

The password guidelines must be followed and cannot be altered.

The implications of not forcing password changes for users could result in loss of personal and very sensitive date. Failure to adhere to this policy could result in criminal investigation, fines or conviction.

Process

The ICT Support Team are responsible for ensuring password policies are configured correctly. Staff members are responsible for ensuring their passwords are of a complex nature and cannot be easily guessed.

Audit/Monitoring/Reporting/Review

The ICT Support Team will ensure that full records are kept of:

- User IDs and requests for password changes
- User logs
- Security incidents related to this policy. In the event of a serious security incident, the police may request and will be allowed access to passwords.
- This policy will be reviewed at least annually in response to changes in guidance and evidence gained from the logs.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

Appendix 1

The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies

- Complaints
- Safeguarding Children and Young people
- Behaviour
- Anti-Bullying
- Lettings and Use of Premises
- Special Educational Needs
- School trips
- Curriculum
- Children in Care
- Health and Safety
- Sex and Relationships Education
- Security
- Equality Diversity and Community Cohesion
- Students with Medical Needs
- Internet Access and Use
- Use of ICT and Website
- e safety
- Young Carers
- Privacy and Confidentiality
- Cloud based
- Digital Images
- Whistle blowing

The above list is not exhaustive but when undertaking development or planning of any kind the school will consider safeguarding matters

- **Revision Notes**

Rev A:	Original agreed and approved by Full Governing Body on 4/07/2018
Rev B:	Agreed and Approved by the Audit, Finance and Premises Committee 11/1/22

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

*Appendix 1

The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies

- Complaints
- Safeguarding Children and Young people
- Behaviour
- Anti-Bullying
- Lettings and Use of Premises
- Special Educational Needs
- School trips
- Curriculum
- Children in Care
- Health and Safety
- Sex and Relationships Education
- Security
- Equality Diversity and Community Cohesion
- Students with Additional Needs
- Internet Access and Use
- Use of ICT and Website
- Young Carers
- Privacy, Confidentiality, Information Sharing and Data
- Whistle blowing

The above list is not exhaustive but when undertaking development or planning of any kind the school will consider safeguarding matters.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)