



# *Windmill Hill Academy*

## **School Password Security Policy 2016**

The An Daras Multi Academy Trust (ADMAT) Company

An Exempt Charity Limited by Guarantee

Company Number/08156955

Status: <b>Approved</b>	
Recommended	
Statutory	Yes
Version	v1.0
Adopted v1.0	
Reviewed and approved as v1.0	<b>March 2016</b>
Next Review	<b>March 2017</b>
Advisory Committee	Local Governing Advisory Body
Linked Documents and Policies	WHA Computing Policy ADMAT Acceptable Use of IT Policy WHA Filtering Policy WHA E-Safety Policy WHA Child Protection and Safeguarding Policy WHA Staff Code of Conduct Policy



# School Password Security Policy 2016

## Introduction

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username/password system is essential if the above is to be established and will apply to all school IT systems, including email and Virtual Learning Environments (VLE).

## Responsibilities

The management of the Password Security Policy will be the responsibility of the IT technician

All users (adults and KS2 users) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users and replacement passwords for existing users will be allocated by the IT technician. Any changes carried out must be notified to the manager of the Password Security Policy (above).

## Training/Awareness

Members of staff will be made aware of the school's Password Policy:

- at induction
- through the school's E-safety Policy and Password Security Policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school's Password Policy:

- in IT and/or e-safety lessons
- through the Code of Conduct for Users/Acceptable Use Policy/Agreement

## Policy Statements

All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Local Governing Advisory Body.

All users (at KS2 and above) will be provided with a username and password by the IT Technician who will keep an up to date record of users and their usernames

The following rules apply to the use of passwords:

- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user*

The "administrator" passwords for the school IT system, used by the Network Manager (or other person) must also be available to the Head of School or other nominated senior leader and kept in a secure place (e.g. school safe).

**Audit / Monitoring / Reporting / Review**

The IT Technician will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- 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 used for encryption.

Local Authority Auditors/External MAT Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

This policy will be regularly reviewed annually in response to changes in guidance and evidence gained from the logs.

Approved by the LGAB – **March 2016**

Next Review – **March 2017**