IT Password Policy

Key Document Details

School Name:	The White Horse Federation – all schools		
Version no:	9	Ratified date:	May 2021
Author:	M Weller	Interim review date	n/a
Owner:	M Weller	Next review date:	September 2022
Approved by:	CEO		

1. Introduction

1.1. Statement

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

1.2. Aim and purpose

The WHFIT Support Team will be responsible for ensuring that the White Horse Federation 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 Principal of the school will be responsible for ensuring that users conform to the policy on a day to day basis.

1.3. Who it applies to

This policy applies to all employees and students of the MAT.

2. Policy

2.1. Description

- 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 WHFIT Support Team and will be reviewed, at least annually.
- All school/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 WHFIT Support Team.
- Passwords for new users will be allocated by the WHFIT Support Team. Replacement network/application passwords will be allocated by WHFIT Support Team or authorised school 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 on details and must immediately report any suspicion or evidence of a breach of security to the schools or departments Information Asset Owner (IAO).
- Users will change their passwords at regular intervals in accordance to guidelines outlined below.
- Requests for staff password changes will be recorded using the WHFIT 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 be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
- The password must not include proper names or any other personal information about the user that might be known by others.
- Where possible please use the three random words process for choosing a password, once you have 3 words ensure you change some letters to numbers, upper and lower case with special characters. The National Cyber Security Centre blog on this can be found here
- The account will 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 60 days.
- Should not re-used for 6 months and be significantly different from previous passwords.

Two factor authentication (2FA)

With the increased threat from phishing and cyber attacks the WHFIT Support Team will be rolling out 2FA to all staff. Please note you will require a mobile device for this.

Student/pupil passwords

- All users from KS2 and above will be provided with a username and password.
- Students/pupils 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 school's online safety policy and password policy
- through the Acceptable Use Agreement.

Pupils/students will be made aware of the school's password policy:

- in lessons when teaching the Computing curriculum
- through the Acceptable Use Agreement

2.2. Permissive/ non permissive

The password guidelines must be followed and cannot be altered.

2.3. Compliance

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

3. Key steps in the process

3.1. Roles and responsibilities

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

3.2. Procedures

Audit/Monitoring/Reporting/Review

The WHFIT 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.

3.3. Local conditions statement

In some circumstances, local conditions mean that delivery will require local specific changes in the procedures. However, the core essence of the policy must be followed.

Please detail below any school specific policy changes, this must be signed by the principal of the school and they are responsible for this change in policy guidelines.
School Password Policy

Authorised Personnel for changing student network passwords:

Name	Position	Reason

Authorised Personnel for changing staff network passwords:

Name	Position	Reason

Authorised Personnel for changing Management Information System staff passwords:

Name	Position	Reason

School Name:

Principal Name:

Signature:

Date: