Woodthorpe J.I. School

Password Security Policy

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

A safe and secure username/password system is established and will apply to all school ICT systems, including email and Woodthorpe Website. The school considers secure passwords to take account of the following:

- a minimum of eight characters and be difficult to guess;
- different passwords to be used for different accounts and applications; and
- should contain numbers, letters and special characters.

Responsibilities

The management of the password security policy will be the responsibility of ICT Technician / ICT coordinator/ Headteacher.

All users (and young people as appropriate) 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 to the Headteacher/ICT Coordinator 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 ICT Technician / ICT coordinator

Users will change their passwords on a regular basis as deemed appropriate.

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; and
- through the Acceptable User Agreement.

Pupils/students will be made aware of the school's password policy in Computing and e-safety lessons.

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee.

Children will be provided with a username and password as appropriate.

All adult users will be provided with a username and password by ICT Technician / ICT coordinator/ administrator who will keep an up to date record of users and their usernames.

The following rules apply to the use of password

- 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 in an identifiable form;
- requests for password changes should be authenticated by ICT Technician / ICT coordinator administrator to ensure that the new password can only be passed to the genuine user/genuine user's teacher; and
- the "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher/School Administrator/ ICT coordinator and kept in a secure place.

Audit / Monitoring / Reporting / Review

The responsible person (ICT technician/coordinator) will ensure that full records are kept of:

- user IDs and requests for password changes;
- user log-ons; and
- security incidents related to this policy will be kept by the Headteacher in the e-safety log.

In the event of a serious IT security incident, the police may request and will be allowed access.

Local Authority Auditors also have the right of access for audit investigation purposes

User lists, IDs and other security related information must be stored in a secure manner. Only accessible using the admin password access and a hard copy in the school safe.

The e-safety incident logs will be reviewed by *E-Safety Governors annually*.
This policy will be regularly reviewed (annually) in response to changes in guidance and evidence gained from the logs.

Signed: ……

Date: March 2018

Review: March 2019