GDPR DATA PROTECTION

PASSWORD POLICY

Mulbarton Primary

GDPR Password Policy

[Version 2019 v1.1]

If you are reading a printed version of this document you should check the Information Management pages on the school network to ensure you have the most up-to-date version.

GDPR DATA PROTECTION

PASSWORD POLICY

Document version control

Version	Author	Date	Approved by	Effective from
1.0 model	DPE – JK	17/6/2018	TK (inc QA).	
1.1	DPE - JW	11/6/2019		

School sign off 06.05.2020

Name	Title	Date
Bev Theobald	Data Protection Lead	06.05.2020
Dan Warncken	Network Manager	06.05.2020
Nicola Wright	Computing Lead	06.05.2020
Kevin Holland	E-safety Governor	06.05.2020

GDPR DATA PROTECTION

PASSWORD POLICY

Contents

GDPR DATA PROTECTION

PASSWORD POLICY

Introduction

The need for a password policy

The purpose of a password is to prevent unauthorised individuals from accessing school data, devices or resources.

Under the GDPR and the Data Protection Act 2018, Mulbarton primary has an obligation to implement technological and organisational measures to show we have considered and integrated data protection into our data processing activities.

"Measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected."

Passwords can be considered one of the appropriate safeguards to ensure the security of accounts and the confidentiality of sensitive information, provided an appropriate password policy is in place.

Scope

A safe and secure username / password system is essential and will apply to all school technical systems, including:

- Networks, devices, email and all internet based programmes.

Who

This policy is applicable for all technical system 'users' e.g. staff (including managers, contractors, volunteers) pupils and governors.

- All individuals, including pupils from KS2 and upwards, that have password accounts to access sites, systems or email on the school computer systems and devices must adhere to the password policies defined below to protect the security of the network/devices and to protect data confidentiality, integrity and accessibility.

School responsibilities

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

- Users can only access data to which they have right of access;
- No user should be able to access another user's files without permission, unless part of a documented monitoring and review policy;
- Access to personal data is securely controlled in line with the school's privacy and personal data protection policy;
- The Headteacher or another nominated senior leader will know details for the school network/system administrator accounts and a copy is also stored in a secure area/safe.

Password security management

The management of the password security policy will be the responsibility of the Computing Lead and the Network Manager. This includes:

- Defining and recording/documenting the access rights available to groups of users;
- Allocating temporary passwords for new users which must be changed by users on first use;
- Setting up rules for what passwords the school systems will accept;
- Setting up security features so that accounts are 'locked' following six successive incorrect logon attempts;
- Providing a secure mechanism for resetting passwords if they have been forgotten or need to be changed for another reason;
- Ensuring that school staff cannot view other user passwords;
- Ensuring that passwords are never displayed on screen and that all stored passwords are encrypted to current industry standards and never stored as plain text or transferred digitally (unless encrypted);
- Implementing two factor authentication procedures using [e.g. a hardware token] when sensitive data is stored on laptops or other mobile devices;
- **Keeping the burden on staff to reset passwords etc to a minimum in order to make it easier to maintain strong passwords, in line with NCSC password guidance:**
  https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Training/Awareness

Members of staff and other adults will be made aware of the school's password policy and best practices:

- At their induction;
- Through general cyber security training e.g. GDPR Data Protection 101 e-learning;
- Through this and other relevant school policy documents;
- Through posters and annual reinforcement activities/resources.

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

- In ICT, PSHE or e-safety lessons;
- By using posters placed near computing equipment;
- In the school Acceptable Use Policy.

Audit / Monitoring / Reporting / Review

The Network Manager will ensure that full records are kept of:

- User IDs and requests for password changes;
- User logons;
- Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to encrypted passwords where available.

These records will be reviewed by the Network Manager, Computing Lead and E-Safety Governor at regular intervals with a minimum of once a year. A review may also occur in response to changes in guidance or evidence gained from the logs.

User responsibilities

Staff and other adult account holders

All staff (and other adult users) have responsibility for the security of their username and password.

All staff users will be provided with a username and a password by the Network Manager who will keep an up-to-date record of users and their usernames.

All new or reset passwords are temporary and must be changed when next logging into the account by creating a 'strong' password as follows:

- Aim for at least 10 characters long, maybe using 4-5 random words;
- Include upper and lower-case letters, a number, a special character;
- Must not contain proper names nor common 'weak' passwords such as password, 123456, qwerty etc, or any personal information that might be known by others.

Passwords should be different for different accounts, and **never** the same as those passwords used outside of school.

User accounts will be 'locked out' following six successive incorrect log-on attempts.

Users should never allow any other users to access the systems using your log on details and **immediately** report any suspicion or evidence that there has been a breach of security to the Computing Lead and network manager;

- Change passwords immediately if there are any concerns of a possible security incident;
- Change passwords every 12 months as defined by this policy;
- When using two-factor authentication, any hardware tokens must be stored separately from the laptop/device, especially when in transit, to avoid both being lost/stolen together.
- Never display passwords on screen or store in accessible/visible places;
- Use training/resources to refresh best practice guidance and risks from hackers such as: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

GDPR DATA PROTECTION

PASSWORD POLICY

Pupils and students in KS 2

- You will be provided with a username and password;
- You have responsibility for the security of your own username and password;
- You will be required to change your password, for example: when you first login or if there are any concerns;
- You will also be required to change your password at set intervals – for example: once a year;
- You need to be aware that a weak password can easily be guessed by criminals/hackers, so you need to use a strong password;
- To make your password strong:
    - Include 10 or more characters, or maybe 4-5 random words;
    - Use a mix of letters, capital letters, numbers and other keyboard characters such as: ! # $ % & * + - / = ? ^ _ ` { | } ~
    - Do **not** use common words, names of people, pets, places, film characters or favourite hobbies;
    - But make something up that you will be able to remember!
- You must **not** allow anyone else to use your log on details and password;
- Contact a member of staff if you need to request a new password (password reset) or if you think your password is being used by anyone else.

Pupils in Early Years and KS1

For pupils up to year 3 class logins will be used.

This type of use by pupils will always be supervised and monitored by the relevant class teachers to ensure rules set out in this policy or the Acceptable Use Policy are not infringed.

Members of staff should never use a class log on for their own network access.

GDPR DATA PROTECTION

PASSWORD POLICY

PUPIL'S PASSWORD AGREEMENT

Complete this form to let your school know that you have read this advice on creating a STRONG password:

A) I will create a STRONG password and keep it safe by …

	PASSWORD DOs	Tick
How Long?	It needs to be at least 8 characters long	
What Letters?	I will use lowercase and UPPERCASE letters	
Numbers?	I will use at least 1 number and…	
Other symbols?	…at least one of these: !@#$%^&*(){}[]	
Can you remember it?	I will think of a way to remember my password	
Reset needed?	I will think of a new strong password using these same rules when I'm asked to change it	
	PASSWORD DON'Ts	Tick
Names?	I will not use my NAME, my family or friends' names or my PET's name in my password	
Easy to guess words	I will try not to use easy to guess words without jumbling up letters and adding numbers	
Secret and secure	I won't give anyone else my password!	

B) If you ticked everything – sign here!

By signing below, you are agreeing to try and follow the password rules of our school:

Name: .....

Signature: .....

Date: .....