Hardenhuish School
School Password Security Procedure

If you would like any policy in a more accessible version, please contact the Administration Manager

Related Policies/Procedures: Data Protection Policy, Password Security Procedure, Information Security Policy, Staff AUP, Pupil AUP, Governor AUP

Contents

1. Introduction

The School needs to maintain the security of its ICT systems and the data stored within them. We use a system of individual user accounts so that the right people have access to the right information. Everyone must use strong passwords and keep them secure to protect these accounts.

This procedure sets out the standards required for passwords used for accounts on any school ICT system and steps you must take to keep them secure. It applies to all staff, volunteers, governors, pupils, and contractors who have access to ICT systems. It is your responsibility to follow this procedure so that your account is kept secure. If you believe there has been a security breach, you must report it at once to the ICT Helpdesk, icthelpdesk@hardenhuish.wilts.sch.uk.

2. Creating strong passwords

When you create your password, it must:

- be at least 14 characters long;
- contain a mix of characters – uppercase, lowercase, symbols, and numbers;
- not be like passwords you currently use for other accounts;
- not be like passwords you've used for any accounts in the past; and
- be easy for you to remember but difficult for anyone else to guess.

Don't use your birthday, names of family members, friends, or pets, etc. that can be guessed easily.

We recommend using a memorable phrase of three or more words. For example, it's easy to remember the image of a giant purple apple but hard for anyone else to guess. This could become *Gi4ntPurp1eaPPl3!* for your password.

3. Keeping passwords secure

Never share your password with anyone. Don't reveal it in an email, on the phone, or through any other system that isn't reliably secure even if you think the person asking is trustworthy. If you suspect anyone else knows your password, you must change it at once.

Never record your password without encryption. You can use a password manager such as the one built into browsers like Microsoft Edge so you don't have to remember too many passwords. Avoid keeping written notes of your password near the device it protects.

Don't reuse your password for any other systems. If a hacker breaks one system, they will be able to access all your other accounts if the password is the same or similar.

Unless you're sure it's trustworthy, don't enter your password into websites. For example, if you click a link in an email and you are asked to log in, only enter your details if you are certain that the email and login page is genuine.

Many systems now require "multi factor" or "two factor" authentication. If this is required, there are different ways of fulfilling this requirement. Most systems now allow the use of an app on a smart phone, such as the Microsoft Authenticator app. Others may require a physical USB token that has to be plugged in. Such a token must be stored separate to the device you will use it with. The lowest security option is receiving SMS messages on any mobile phone. It is inadvisable to use this option, and services are starting to remove this option.