Password Policy and Guide

Employees at Wolfson College access a variety of IT resources, including data, computers and other hardware devices. Passwords are a key part of our strategy to make sure only authorized people can access them.

All employees who have access to any of those resources are responsible for protecting their log-in information from unauthorized people.

The purpose of this policy is to make sure all Wolfson College resources and data receive adequate password protection. The policy covers all employees who are responsible for one or more account or have access to any resource that requires a password.

1. Password for Workstation and Role based Hermes Email Account

   a. Get a password from the IT Office if you do not have one.
   b. Once you are given a password, do not change it without first consulting the IT Office. The IT Office keeps a record of workstation and Hermes passwords. It does not include personal email accounts.

2. Passwords for Raven and other accounts within or outside the University

   a. All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. Longer passwords are even better (12-14 characters).
   b. In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. Choices like "password", "password1" and "Pa$$w0rd" are equally bad.
   c. A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember 50th anniversary" can be turned into TmB0WTr50a!. Here is a Strong Password Guide Site.

An example of a good password.

!@*&u3@*A% &$*@!#b$2*!

   http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it

   d. Another method is to combine at least 5 random words into a reasonably long phrase consisting of at least 30 characters such as PurpleSheep2MowerCityLuxury
   e. If an employees can change their password for external sites on a regular basis without the need to write it down then this is recommended. However, this is not recommended for workstation and work email accounts (see the section 1 above)

f. If you need any help with setting of changing passwords, please contact the IT Office at helpdesk@wolfson.cam.ac.uk

3. Protecting passwords

a. If the security of a password is in doubt, for example, if it appears that an unauthorized person has logged in to the account, the password must be changed immediately. The IT Office must be informed if this happens.

b. Do not write passwords down or keep them at their workstations.

c. Do not use password managers or other tools to help store and remember passwords. Saving passwords in an electronic file MUST also be avoided.

d. Do not share your password with anyone else including co-workers unless required for a College purpose and approved by the IT Office.

e. Do not share your password with any outside party, including those claiming to be representatives of a business partner with a legitimate need to access a system. If it is necessary for a business purpose, please consult the IT Office first.

f. Avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees will receive training on how to recognize these attacks. Useful information in this matter is given on the following site.

   http://www.itmanagerdaily.com/spear-phishing-attacks/

g. Never send a password through email. Instead, use other methods like a phone call or mobile Text/SMS message.

Hacked French network exposed its own passwords during TV interview from Post-It notes on wall.