Harvest Private School
RAK. UAE
Email :harvestp.school@gmail.com

Learner-based high-quality education

مدرسة هارفست الخاصة
رأس لخيمة

Password Protection Policy

HPS Password Policy:

- ✓ *Created November 2020 – by ICT department*
- ✓ *Reviewed February 2021- by OSG*
- ✓ *Updated* March 2021- by OSG
- ✓ *Updated April 29, 2022 – by OSG*

Cambridge Assessment International Education
Cambridge International School

Pearson

Creating and using strong passwords

Among the most important ways to ensure the safety of your online interactions is to protect yourpasswords.

The good news is that you can take control of protecting your passwords - you only need to createstrong passwords then keep them secret.

Follow these tips to keep your passwords out of the wrong person's reach.

Create strong passwords

Password security starts with creating a strong password. A strong password is:

- It is at least 12 characters long, but it is better if it is 14 or more.
- A combination of upper and lower case letters, numbers and symbols.
- Not a word that can be found in a dictionary.
- Not the name of a popular person or entity such as a public figure, product, or organization.
- Totally different from previous passwords.
- Consider using a phrase like "6 ^" MonkeysLooking.
-

Secure your passwords

Once you create a strong password, you must follow these instructions to keep it safe:

- Do not share a password with anyone. Not even a friend or family member.
- Do not send a password via email, instant message, or any other method of reliably insecurecommunication.
- Use a unique password for each website. If someone steals a password that you use on multiplewebsites, the information which is protected on all of these sites is at risk.
- If you do not want to remember multiple passwords, you should use a password manager. Passwordmanagers will automatically update stored passwords and keep them encrypted and require multi- factor authentication to access them.

Do not save a password on a device that is designed to protect.

It is okay to write down your passwords, as long as you keep them confidential.

Do not write it on sticky notes or cards close to things your password will protect, even if you think theyare well hidden, or just as a hint..

Instead of jotting down your password on a sheet of paper, consider jotting down a tip that reminds youof what the password is. So if the password is "Paris4SpringVacation!", you can write down your "favorite trip."

Whenever possible, change passwords immediately on accounts you suspect or believe the passwordcould be compromised.

Avoid entering your password on any device if you are not sure whether that device is safe.

These devises that are shared or available for public use may contain installed keylogging programs that allow capturing your password as you type it. You should also avoid allowing your password to besaved on shared or public computers.

Hint

If you are asked to create answers to your security questions, enter a related answer.For example, if the question is "Where were you born?" answered "green".

Answers like these can’t be found Facebook or Twitter by tracking, All you need to do is to insure itsmeaning to you, in order to remember it.

Don't fall victim to divulging your passwords

Criminals can try to hack your password, but sometimes it's easy to exploit human nature and deceptionto reveal it. You are more prone to phishing messages that appear original.

(You may receive an email claiming to be from an online store) like Amazon) or eBay or a phone callfrom "The bank" is trying to convince you of the "legal" need for your password or other sensitiveinformation).

It might be a phishing scam.

Here are some guidelines to follow to protect your passwords and other sensitive information:

In general, beware of anyone requesting of sensitive information from you, even if it issomeone you know or a company you trust.

For example, a fraudster might steal a friend's account and send an email to everyone in anaddress book that belongs to this friend.

Handle all requests for sensitive information with care.

Do not share your password in response to an email or phone request - for example, to verifyyour identity, even if it's from a trusted company or someone.

You can always access websites with always reliable links.

Phishers can copy the look of communications of the company to trick you into clicking on afake link or attachments, so be careful of links that appear in unsolicited emails, instant messages, or SMS.messages.

In case you have any doubt, go straight to the bank's website or other service that you are trying to access while pointing through your own bookmark or by typing the legitimate addressof the service yourself.

Passwords have to consist of the following requirements/standards:

Minimum Length	**(12 – 18) characters.**
Expiration	**90 days.**
Password History	**20** password changes are required before reusing a previous password.
Minimum Password Age	**24 hours**
Lockout	**After 25 attempts**
Complexity or Composition	Must contain **at least three** of the following types of characters: 1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters) 2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters) 3. Numerals (0 through 9) 4. Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ 5. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages. • **The password cannot contain the user's first name, middle name, last name, or username.: o For example, the name "Erin M. Hagens" is split into three tokens: "Erin," "M," and "Hagens." Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password.

Rules to Live By	• **NEVER share your password** • **Do NOT write down your password *unless* you adequatelysecure it** • **Never choose an easy-to-guess password**

Future schedule for reset the students' account password on Microsoft teams:

The ICT department have to reset the Microsoft teams password every 3 months

Month	Responsible
February	ICT Department
May	ICT Department
September	ICT Department

Reset Schedule for the students' accounts passwords

Grades	Responsible
KGs, GR1, GR10,GR11	Ms.Naseem
GR6, GR7, GR8	Ms.Hala
GR2, GR4 , GR5, GR9	Mr.Anas