Password Security Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All Students and staff, including contractors and vendors with access to Crown Private School systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Every user will have an individual secure password access to school systems.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords, and the frequency of change.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at Crown Private School facility, has access to the CPS network, or stores any non-public information under CPS domain/network.

4. Policy

4.1Password Creation

How to choose a strong password? Here are some guidelines for choosing a strong password for your account

- The password must be between 8 and 20 characters.
- The password must:
    - Contain **UPPERCASE** characters (**A through Z**).
    - Contain **lowercase** characters (**a through z**).
    - **Numerals** (0 through 9).
    - Contain **special characters (%!&@ etc.)**

4.1.1 All user-level and system-level passwords must conform to the Password Creation Guidelines (4.1).

4.1.2 It is good to use a separate, unique password for each of their work-related accounts.

4.2 Password Change

4.2.1 All system-level passwords (for example: laptop, Tablet, etc.) must be changed on at least aquarterly basis.

4.2.2 All user-level passwords (for example, email, ERP, LMS, etc.) must be changed at least every 4months. The recommended **change interval is every 3 months**

4.2.3 Every user should mandatorily change the initial account password obtained from ITHelpdesk/System

4.2.4 **Expiration of passwords**: Your system password **will expire automatically every 90 days**. Pleaseset a new password when you see the expiration message.

Students and Staff using school email accounts will receive the **password expiration alert** 30 days priorto the date of expiration.

4.2.5 **Phishing protection**: Failure to enter correct password for emails for 4 consecutive times mayresult in your account being blocked. Please contact IT Helpdesk to enable the account.

4.3 -Password Protection

4.3.1NETWORK ADMINISTRATOR CREDENTIALS

- The IT administrator should store all the IT administrative credentials printed in a secure storage place in the office of the principal.
- The IT admin should update this document regularly

4.3.2 PASSWORD PROTECTION GUIDELINES

- **Use 2 factor authentication** for extra security.
- Add a secondary email and phone numbers to recover the passwords
- Create login notifications to get the alerts for unsuccessful or unauthorized logins
- Passwords must not be shared in email messages.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without protection.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must immediately change the password and report to CPS ITHelpdesk.

4.3.3 USE OF PASSWORDS AND PASSPHRASES

- A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters insertedthroughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember.

For example, the passphrase

- I 1ove my puppy!!!
- My pAssw0rd is $uper str0ng!" is 28 characters long and includes alphabetic, numeric and special characters.

A Pass Phrase is highly recommended for young learner or all students

It is also relatively easy to remember. It is important to note the placement of numeric and symbolic charactersin this example as they prevent multiple words from being found in a standard dictionary. The use of blank spaces also makes a password more difficult to guess.

All of the rules above that apply to passwords apply to passphrases.

4.3.4 ENFORCED PASSWORD CHANGE

1. Users will not be able to reuse a password that had used earlier
2. All the system level and user level password will be required to change every 90 days. Passwords changes are enforced through policy

5. Password Recovery

5.1.1 Stake holders at crown private school should contact relevant staff for

- Password Reset
- Breach of password security
- Access to the password secured systems
- To Enable/Disable access to the CPS Network systems and Applications.

TYPE	STUDENTS (Whom to contact)	PARENTS (Whom to contact)	STAFF (whom to contact)				VISITORS
			SMT	HOD	TEACHERS	ADMIN	
Email	Class Teacher	Teachers	ITHELPDESK	ITHELPDESK	ITHELPDESK	ITHELPDESK	NA
LMS	Class Teacher Subject Teacher	Class Teacher Subject Teacher	ICT In charge	ICT In charge	ICT In charge	IT Helpdesk	NA
Local data Storage	ICT Teacher	NA	IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk	NA
WI-FI	Class teacher	IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk
Cloud Data storage	Class Teacher ICT Teacher	ICT In charge IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk	NA
Network Devices (Eg: Printers)	NA	NA	IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk	NA
Desktop/ Laptop	In Comp Lab ICT Teacher	NA	IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk	NA
BYOD	Subject Teacher	NA	IT Helpdesk	IT Helpdesk	IT Helpdesk	IT Helpdesk	NA

CONTACT DETAILS

IT HELPDESK: Mr. Rajeesh : it@cpschool.uk Contact Number: 067423222 (Extn: 211)

ICT In charge: Ms.Dhanya Dhanya@cpschool.uk

6. TRAININGS

Training to Students and Staff are scheduled as follows

STUDENTS	STAFF
Password protection ideas will be encouraged and shared with students during the e safety lessons and trainings	At the beginning of the new school year during staff orientation
Regular reinforcement is provided in schools ICT curriculum by the ICT Teacher and through the wallpapers and screensavers in the ICT Labs	During the induction training when a staff join the school, any time during the school year
Through posters and Social media and all learning platforms	Trainings provided in weekly Professional developmentprogram.
Awareness through school communication mobile application	Through e safety posters and display wallpapers in the campus
Through circulars and news letters	

PARENTS	VISITORS/ SCHOOL COMMUNITY
In beginning of the school year, basic training is provided during the parent orientation program.	Through posters and videos posted regularly on Social media about the e safety
Parents are encouraged to read the policies on CPS School website. Online safety policy and other e safety policies are included in the website	Through the school websites. Policies one safety is readily available on the websites to read
Through posters and videos posted regularly on Social media	
Awareness through parent mobile application	
Through circulars and news letters	

EDUCATORS NOTES

1 . BE SAFE- Help children understand personal information and how it can be protected

Message 1: Play with the games and apps that are yours.
Devices should be set up so children know which content is for them and that other games, programs or appsmay not be suitable for them. The screen image shows the folder where the little girl can find the games and apps just for her use.

Message 2: Only talk with people you know.
This picture reminds children that they should only video call when a grown-up is helping them, and onlyspeak to people they know.

Message 3 – Some things should be kept private.
In this picture the boys are creating an avatar with their Grandad. Avatars can be a practical way of showingchildren how they can keep their real name and identity private by creating a character to represent themselves in games.

Key questions when discussing this poster could include:

- Do you play on your Mum or Dad's phone, tablet or computer? Do you have a special place for your gamesand apps? How do you know what is yours?
- Do you talk on the computer to your friends and family? Who helps you?
- Why do you think the boy in the last picture looks confused? If you were going to create an avatar foryourself what would it look like? Why?

2 . BE KIND- Teach children to be kind and respectful in digital contexts.

Message 1: Say kind things
Choosing to say kind things when connecting online is a life-long skill that can help prevent cyberbullying later on. The screen image can be a stimulus to discuss the types of things you should do when video calling,like saying hello with a smile.

Message 2: Take turns
Taking turns is a good way of managing time on screens and building self-regulation skills. The child in thebackground of this picture is sad because they have been left out of the game.

Message 3: Ask before you take a photo.
The little boy in is taking a photo of himself with his family. The screen image depicts another time when heis asking his family if they would like to be in the photo.

Key questions when discussing this poster could include:

- Have you ever called your family or friends on a computer or tablet like the people in the first photo? Whatdo you think they are saying? How do you know?
- Why do you think the boy in the middle photo looks sad? What could they do to stop him feeling sad?
- Do you always ask someone if it is OK to take their photo before you take it? Why?

.

3 . ASK FOR HELP- Teach children to ask a trusted grown-up for help with any issue using digital technologies.

Message 1: Tell a grown-up.
It is really important for children to know that if something makes them feel worried, scared or sad whenthey are using a device they should tell a grown-up.

Message 2: Check before you tap.
Before children use a device, they should ask a grown-up. The picture shows the little boy asking if he canplay a new video he has not seen before.

Message 3: You won't get in trouble.
When children are playing with digital technology often things happen that they didn't expect. It can be thesame for grown-ups too! Children need to know that if something unexpected happens, they should tell agrown-up. They should be assured that the grown-up will know it was important for the child to share the problem even if it happened because they made a mistake.

Key questions when discussing this poster could include:

- Have you ever seen something that made you feel worried, scared or sad when you were playing on a tablet? Who would you tell? What do you think they would say?
- Who do you ask before you play, watch or tap on something new on a device?

4 . MAKE GOOD CHOISES- Help children to think about the content they watch and how to manage their time on screens.

Message 1: Why do you like it?
Choosing to say kind things when connecting online is a life-long skill that can help prevent cyberbullying later on. The screen image can be a stimulus to discuss the types of things you should do when video calling,like saying hello with a smile.

Message 2: Use devices near a grown-up
Children need to be aware that digital technologies should be used with a grown-up nearby and in a sharedspace. Children should get used to the idea, from an early age, that devices should not be used in bedrooms.

Message 3: Time's up.
It is important to discuss with children how they will know when it's time to turn devices off and how theywill transition to another activity.

Key questions when discussing this poster could include:

- What do you like to play on devices? What makes you like it?
- Where are these people using devices? Where are you allowed to use them?
- Have you ever been told you have been playing on a device for too long? How do you feel when thathappens? What do you usually do?

8. POLICY COMPLIANCE

An employee or student found to have violated this policy may be subject to disciplinary action

Last updated	Responsible	Summary of change
AUG 2024	Rajeesh Kumar R Online safety coordinator	1. Password enforcement 4.3.4 2. Added User responsibilities (AUP)

User Responsibilities – Acceptable Use Policy (AUP)

Even though you yourself may not store any confidential data on your own PC, your account could serve as a gateway for attackers to access sensitive data on other machines on our internal network, or even compromise the functioning of the CPS Network system as a whole

The login/password combination identifies you as an **individual person**. You are responsible for all activities carried out under your login name and **you must not give out your password to anyone else**

All members are forced to change their initial computing account password at first login. To increase the protection of your account on the CPS network, you will be required to use strong passwords that do not match your previous passwords

You can change your Password at any time following the CPS Password Protection Policy . Weak passwords are one of the easiest ways for hackers to break into a computer. Passwords that are used for years at a time, or passwords that are reused frequently, are also much more likely to be discovered by an attacker.

REQUIREMENTS

Complexity requirements for "strong passwords" are based on the following rules:

- The password is between 8-16 characters' long
- The password contains characters from 3 of the following 4 categories:
  - standard uppercase characters (A - Z)
  - standard lowercase characters (a - z)
  - numbers (0 - 9)
  - symbols: only from among ! % - _ + = [ ] { } : , . ? < > ( ) ;
- The password does not contain your account name or any part of your full name

- The password does not contain characters only found on a particular national keyboard (e.g. ö, ë, å, ñ, é)

- The login (computing account)/password combination identifies a single individual and is reserved for that individual, who is personally responsible for it.
- Passwords must conform to the complexity requirements as per the CPS Password protection policy
- Passwords should never be disclosed and it is strongly suggested that users change their password frequently, at least every 3 months.
- Passwords should not be composed of names or other terms easy to guess or generate automatically (such as any dictionary entry).
- It is recommended that you adopt passwords which are easy to use even when changing from QWERTY and AZERTY to other keyboard layouts.
- Never leave computers unattended while logged-in.
- Information containing one's password should never be stored locally on any commonly accessing computer (ICT Lab computer, internet café, etc.) .
- Users should not attempt to deal with hackers or hacking themselves but should instead report any suspicious activity to the IT administrator preferably to the nearest ICT Service staff.

CONSEQUENCES OF MISUSE

- **CPS Staff/ Students/ Parents as well as Guests** infringing the above rules and regulations face sanctions which may vary from temporary suspension to termination of service(s) or of the personal computing account itself.
- In the event of significant or repeated violation of the present guidelines, the Head of the ICT Service will lodge a complaint to the disciplinary Committee of the CPS according to the Disciplinary Regulations.
- Because of its potentially serious consequences for the work and well-being of the Institute, hacking will be generally regarded as gross misconduct. Where hacking is a criminal offence, offenders may also be liable for criminal prosecution.
- Violation of copyright held by individuals and corporations or other entities can result in civil and criminal liability on the part of the infringer. Also, distribution of Internet viruses, worms, and Trojan horses can lead to civil and/or criminal liability.