CYM

THE INSTITUTE FOR CHILDREN, YOUTH & MISSION

COMPUTER USE POLICY

cym.ac.uk

hello@cym.ac.uk
0115 7770102

Charity No. 1081144

Policy name	Computer Use Policy
Purpose of policy	To cover the minimum specification for hardware and software, with guidelines on the use of social media whilst staff are associated with CYM.
Approval given by	Chief Executive Officer
Last review date	August 2022
Review due date	August 2024
Responsible for review	Chief Executive Officer

1. Introduction

1.1. This computer use policy covers the minimum specification for hardware and software, with guidelines on the use of social media whilst staff are associated with CYM. Most users employ their own computers on home networks, so the policy also covers Bring Your Own Device provisions, in particular with regard to security and compliance, as antivirus and other security software must be kept up-to-date. The policy also includes provisions for the use of the system and file access and storage arrangements in SharePoint and Microsoft Teams.

2. Scope

2.1. This policy applies to everyone who uses CYM's IT infrastructure and/or equipment and the aim of it is to explain acceptable computer use. CYM's email and internet is provided during working hours and your use must comply with all organisation policies and procedures.

3. Confidential Data

3.1. Confidential data is valuable and is to be kept secret. CYM confidential data includes:

3.1.1. Unpublished financial information

3.1.2. Data of customers/partners/vendors

3.1.3. Patents, formulas or new technologies

3.1.4. Customer lists (existing and prospective)

3.2. You are obliged to protect this data.

3.3. Security measures are put in place to:

3.3.1. Protect information from unauthorised access or misuse.

3.3.2. Ensure the confidentiality of information.

3.3.3. Maintain the integrity of information.

3.3.4. Maintain the availability of information systems and information for service delivery.

3.3.5. Comply with regulatory, contractual and legal requirements.

3.3.6. Maintain physical, logical, environmental and communications security.

3.3.7. Dispose of information in an appropriate and secure manner when it is no longer in use.

4. File access and storage arrangements in SharePoint and Microsoft Teams

4.1. You will be granted access to those SharePoint folders/Microsoft Teams teams you need to manage your work. In all cases, CYM files must be accessed, worked on and filed in SharePoint or Microsoft Teams – do not save CYM files to the device you are using.

5. Personal and company devices

5.1. When you use your own digital devices to access company emails or accounts, you introduce a security risk to company data. You must keep both your personal and company-issued computer, tablet and mobile phone secure.

5.2. The computer you use for your work with CYM must have the current supported version(s) of the Windows operating system and Microsoft 365 for Business (Education Edition). You must also have approved anti-virus software installed and the Windows Defender (or other approved) software firewall enabled.

5.3. You must set your computer to update automatically when software or hardware manufacturers issue patches and updates. IT support can assist you in this respect.

5.4. If installed, you must not disable any remote management and monitoring software.

5.5. If you work from home, your internet access via your home router must not use a manufacturer's default name and/or password. You will be provided with support as to how to change the defaults.

5.6. In addition, to keep your device secure, make sure you do the following:

5.6.1. Keep all devices password protected.

5.6.2. Do not leave devices exposed or unattended.

5.6.3. Lock your device when you are not at your desk (Ctrl Alt Del)

5.6.4. Do not access CYM systems from other people's devices.

5.6.5. Do not lend your device to others.

6. Managing passwords

6.1. Password leaks are a major security risk, since they can compromise CYM's entire infrastructure. Not only should passwords be secure so they will not be brute-forced easily, but they should also remain secret. For this reason, you must:

6.1.1. Choose passwords that conform to the schema below – with a minimum length of 15 characters, including capital and lower-case letters, numbers and symbols.

6.1.2. Avoid information that can be guessed easily (e.g. birthdays)

6.1.3. As you require a different password for each service you use – remembering passwords becomes impossible.

6.1.4. It is possible to keep a paper copy of passwords, but this is discouraged. Encrypted digital solutions are more secure. Reputable online password banks and encrypted Microsoft Word, Excel or OneNote documents are approved password digital storage

6.1.5. Do not share your passwords unless instructed by a senior manager who has the authority to issue the

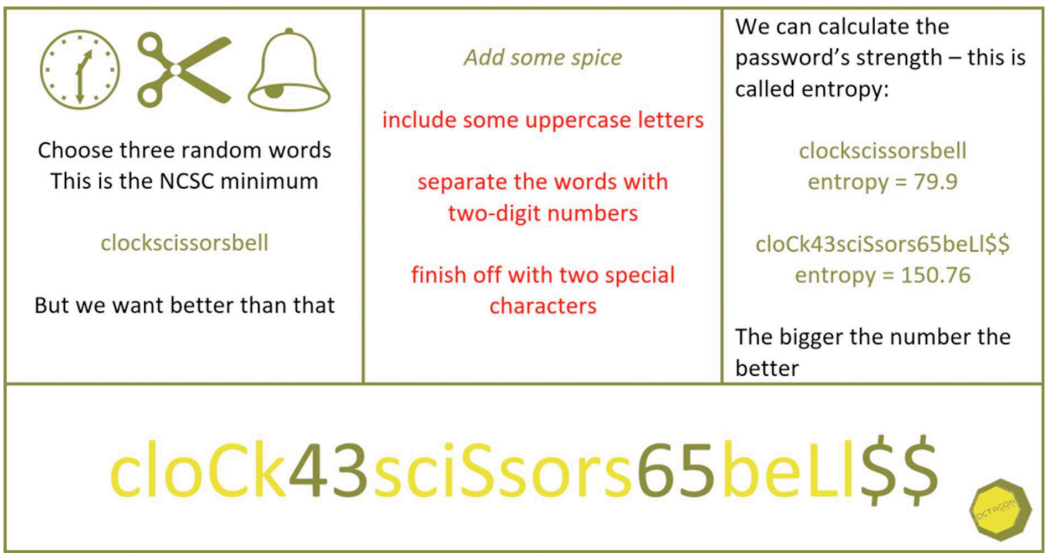
6.1.6. instruction

6.1.7. Use a unique password for your CYM account.

6.1.8. If you believe your password has been compromised, change the password and then report the suspected compromise to your line manager, who will inform IT support

6.1.9. Change your password if IT support issues you with an instruction to do so

6.2. Structure of secure passwords: The following is provided as a guide for secure passwords:



6.3. Multifactor authentication using your phone should be enabled whenever possible. Never share a one-time password.

7. Data transfers

7.1. Transferring data introduces security risk. You must:

7.1.1. Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, please ask IT support for help

7.1.2. Share confidential data over the CYM network/system and not over public Wi-Fi or private connection

7.1.3. Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies

7.1.4. Report scams, privacy breaches and hacking attempts

7.2. IT support need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, please report perceived attacks, suspicious emails or phishing attempts as soon as possible to your line manager, who must investigate promptly, resolve the issue and send a CYM-wide alert when necessary.

7.3. IT support are responsible for training employees on how to detect scam emails. We encourage you to contact them with any questions or concerns.

8. Additional measures

8.1. To reduce the likelihood of security breaches, you must:

8.1.1. Turn off your screen and lock your devices when leaving your desk, including when working remotely.

8.1.2. Report stolen or damaged equipment as soon as possible to your line manager.

8.1.3. Change all account passwords at once when a device is stolen.

8.1.4. Report a perceived threat or possible security weakness in CYM systems.

8.1.5. Not download suspicious, unauthorised or illegal software on your CYM equipment

8.1.6. Not access suspicious websites

8.2. IT support will:

8.2.1. Control access to the global administrator accounts in conjunction with CYM management

8.2.2. Install firewalls, anti-virus software and access authentication systems as required.

8.2.3. Follow these policies provisions as other employees do.

8.3. Cyber security support will:

8.3.1. Arrange for security training for all employees.

8.3.2. Inform employees regularly about new scam emails or viruses and ways to combat them.

8.3.3. Investigate security breaches thoroughly.

8.3.4. Carry out these tasks in conjunction with IT support.

8.3.5. Follow these policies provisions as other employees do.

9. Disciplinary action

9.1 You must always follow this policy, and those who cause security breaches may face disciplinary action:

9.1.1. Unintentional, small-scale security breach: we shall arrange further training on security for you

9.1.2. Intentional, repeated or large-scale breaches (which cause severe financial or other damage): we shall instigate disciplinary action up to and including termination

9.2. Each incident will be examined on a case-by-case basis.

9.3. Additionally, if you are observed to disregard CYM's security instructions you will face progressive disciplinary action, even if your behaviour has not resulted in a security breach.

END