Chiltern Way Academy

Turning Futures Around

Information Technology (IT) Policy

Responsibility for this policy (job title): IT Manager

Responsibility for its review: CEO

Approved: 11.12.2020

Next Review Date: Autumn 2021

Table of Contents

Information Technology (IT): Overview

The purpose of this Information Technology ("IT") policy and procedures is to establish guidelines for the use and management of IT equipment (workstations, servers, printers, etc.) by the Chiltern Way Academy (CWA) and for the implementation of a level of security which will provide for the protection of data and information technology resources from accidental or intentional unauthorised disclosure, modification, or destruction by persons within or outside the company.

To better serve our staff and students and provide our employees with the best tools to do their jobs, CWA makes available to our workforce, access to one or more forms of electronic media and services, including computers, e-mail, telephones, voicemail, mobiles and online services.

To ensure that all employees are responsible, the following guidelines have been established for equipment within CWA. No policy can lay down rules to cover every possible situation. Instead, it is designed to express CWA's philosophy and set forth general principles when using electronic media and services. As the CWA continues to grow, that need may arise and CWA reserves the right to revise, supplement, or rescind any policies or portion of the policies from time to time as it deems appropriate, and its sole and absolute discretion. Employees will, of course, be notified of such changes to the Policies as they occur.

1.1.1 - Prohibited Communication

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene, sexually explicit or pornographic;
- Defamatory or threatening;
- In violation of any license governing the use of software; or
- Engaged in for any purpose that is illegal or contrary to Chiltern Way Academy's policy or business interests.

1.1.2 – User Access

Access to CWA's servers and system resources by employees or outside sources will be determined by the IT Manager in coordination with the CEO. Existing laws and regulations and each staff's position requirements will be taken into consideration in determining the staff's level of access.

- An electronic log will be kept listing those individuals who have access and a list of the authorisations they have been granted.

1.1.3 – Email and Internet Usage

The computers, electronic media and services provided by CWA are primarily for business use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. Incidental personal use is permissible so long as:

- It does not consume more than a trivial amount of resources.
- It does not interfere with staff productivity.
- It does not pre-empt any business activity.

However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

All employees and contractors are given a specific username and specific credentials to the server to accomplish their job responsibilities. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to responsibility for actions the other party takes with the password. If users need to share computer resident data, they should utilise message-forwarding facilities, public directories on local area network servers, and other authorised information-sharing mechanisms. To prevent unauthorised parties from obtaining access to electronic communications, users must follow the Password Policy (1.1.4) in place.

Employees are reminded that CWA's electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data, the employee must see the IT Manager for assistance.

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. CWA is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, CWA also

is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

CWA cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

It is the policy of CWA **not** to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that CWA will, from time-to-time, examine the content of electronic communications.

Recognising that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. CWA sensitive information **must not** be forwarded to any party outside CWA without the prior approval of the CEO. Blanket forwarding of messages to parties outside CWA is prohibited unless the prior permission has been obtained.

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. CWA has processes and systems in place to archive emails based upon standards set forth with the retention policy. More information can be discussed with your line manager about the retention policy. If Chiltern Way Academy is involved in a litigation action, all electronic messages pertaining to that litigation will be placed in legal hold and not deleted until CWA's CEO or designated representative has communicated that it is legal to do so.

1.1.4 – Password Policy & Management

In order to have access to the company's IT resources (e-mail, servers, workstations, printers) all users must obtain a user account from CWA's IT department. Once the account is established, users will set their own passwords to gain access to those resources.
The organisation's Password Policy applies to all employees, contractors, temporary workers, volunteers and others that operate organisation-provided computers, access organisation-provided Internet services or access organisation-provided electronic mail services. All use of the organisation's user accounts, desktop computers, notebook PCs, servers, Internet services and electronic communications must conform to the guidelines presented in this policy.

Passwords are required for the network account, e-mail account, server access and any other account the user may be assigned to. Although this is not a requirement, preferably each account should have a different password.

- Should the IT department ever need to change the user's set of passwords in order to access the account information, the user, his or her line manager, the network administrator, the CEO and the Head of Campus should be notified of this fact as soon as possible. In this case, the old passwords will be invalidated and the user should immediately establish a new set of passwords.

- If there are reasons to suspect a password has been compromised, the network administrator has the authority to disable an account or change a user's passwords, temporarily suspending user access to the account(s). In such cases, the CEO the Head of Campus, the user's line manager and the user will be notified as soon as possible.

Password Management

Passwords for various systems have rules defined such as password expiration, uniqueness, minimum characters, whether the password must contain a combination of alphabetic, numeric and special characters, whether passwords are case sensitive etc. Passwords for all systems are never to be revealed to anyone else and are subject to the following rules:

- No passwords are to be spoken, written, e-mailed, hinted at, shared or otherwise made known to anyone other than the user involved.

- No passwords are to be shared in order to "cover" for another individual who is out of the office or otherwise indisposed. Instead, contact the Information Technology department for a temporary account or other access

- Passwords should never be physically written on paper nor written and concealed near a workstation.

- All computers and servers should use the operating system's screen saver feature and require the user account and password to be entered to regain access when the system is left idle for any period longer than three minutes.

- Passwords should never be reused, dependent on system this may be a default setting.

Password Complexity

Passwords for all end user windows/email must meet the following criteria:

- Passwords must be at least five (5) characters in length.
- Passwords must contain both letters and numerals.
- Passwords must include mixed cases (both capital and lowercase letters).
- Passwords must include at least one (1) numeric.
- Passwords can include symbols: (i.e. !, @, #, $, %, ^, &, *,).
- Passwords must not include any portion of your name, address, date of birth, Social Security Number, username, nickname, family name, pet name, sports team nameor word that appears in a dictionary or any such word spelled backward.
- Passwords remembered on server is (3) last passwords, cannot repeat password.
- Passwords are required to be changed every 90 days.

Passwords for all administrative and financial systems must meet the following criteria:

- Passwords must be at least six (6) characters in length.
- Passwords must contain both letters and numerals.
- Passwords must contain mixed cases (both capital and lowercase letters).
- Passwords must include at least two (2) non-alphanumeric symbols:(i.e. !, @, #, $, %, ^, &, *,).
- Passwords must not include any portion of your name, address, date of birth, Social Security Number, username, nickname, family name, pet name, sports team nameor word that appears in a dictionary or any such word spelled backward.
- Passwords should be changed every 120 days unless other needs are required(i.e. database)

Systems Covered

The Password Policies guidelines apply to all departments, divisions, locations employees, contractors, temporary workers, volunteers and others that operate organisation-provided accounts, equipment and services, including the following:

- Network and operating system user accounts
- Web accounts
- E-mail accounts

1.1.5 – Access to Employee Communications

Generally, electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voicemail, telephones, Internet and bulletin board system access, and similar electronic media is not reviewed by CWA. However, the following conditions should be noted:

- It may be necessary for staff to review the content of an individual employee's communications during the course of problem resolution. No staff may review the content of an individual employee's communications out of personal curiosity or atthe behest of individuals who have not gone through proper approval channels (CEO, HR, etc.).

- CWA can routinely gather logs for most electronic activities or monitor employee communications directly, e.g., telephone numbers dialled, sites accessed, calls received, and time at which calls are made. CWA reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other company policies.

- Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

1.1.6 – Software Installation and Management

It is CWA's policy that the members of the IT department are the only persons authorised to install, update or remove software from a workstation, to add or remove printers or, in general, to change workstation settings. On a case by case basis, other staff members may be authorised by the network administrator to perform these tasks.

- It is CWA's policy to ensure that all software installed on computers that are property of the CWA is either in the public domain or has been legally purchased or leased by CWA.

- It is CWA's policy that any software found installed on a workstation which violates the policies stated in this section will be immediately deleted upon detection.

- The IT department will assign each server, workstation, laptop or notebook an administrator password that will be known only to the members of the IT department.

- The IT department will then establish user profiles in order to protect the programs and data in a workstation from being accidentally or intentionally deleted by users, prevent the installation of non-authorised or conflicting software, prevent usersfrom

saving information to specified locations, prevent the access, installation or removal of printers and other hardware and, in general, prevent users from changing a workstation's configuration.

- The IT department staff are the only persons authorised to install, update or remove software from servers and workstations, to add or delete printers and, in general, to change workstation settings.

- The IT department staff will review periodically the software installed in company workstations to ensure that all the software has been legally purchased or leased by CWA.

- The IT department will keep a log of installed software to make sure that the number of licenses purchased or leased is not exceeded.

- If it is determined that a staff member has violated company policy by installing illegal or unauthorised software, this fact will be reported immediately to the CEO, the staff's line manager and the Head of Campus – who will decide the appropriate course of action.

1.1.7 – Saving User Data to Server

Each member of CWA staff will be assigned a specific network drive to store their work. Users will be made aware that they must save their documents only to their designated network drives.

- No client protected information should ever be stored in personal folders. Shared Network Folders are setup on the server for this purpose.
- No personal photos, videos or music are to be stored on the server.

1.1.8 – Hardware

All hardware devices acquired for or on behalf of CWA are and shall be deemed company property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

All purchasing of computer hardware devices shall be centralised with the IT department to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price. All requests for computing hardware devices must be submitted to the Head of Campus for approval. The request must then be sent to the IT department, which will then determine standard hardware that best accommodates the desired request and obtain proper purchasing approval.

No outside equipment may be plugged into the company's network without the IT department's permission. This includes USB drives in computers. Personal computers can access the employee Wi-Fi only.

1.1.9 – Purchasing

Software – All software that is required must be approved by department manager and the IT Department. All software required for employee to perform work tasks should be discussed with the IT department to ensure the correct software is being purchased or that CWA does not already own necessary licensing. Once department manager has approved software the IT department will request approval and purchase software.

Hardware – All hardware that is required must be approved by department manager and the IT department. Once department manager has approved hardware requirements the IT department will request approval and purchase hardware and configure per managers request.

1.1.10 – Security/Appropriate Use

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorisation has been granted by management, employees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties;
- Hacking or obtaining access to systems or accounts they are not authorised to use;
- Using other people's log-ins or passwords; and
- Breaching, testing, or monitoring computer or network security measures.

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic assets/materials of other companies' or individuals' must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

1.1.11 – Security Incident and Response Reporting

It is CWA's policy to ensure that no protected information is electronically submitted unnecessarily.

Should information need to be transmitted, information will be password protected before being sent. The password is then sent as part of a separate email and/or the person is notified of password verbally through a phone call.

Confidentiality Notices such as the following will be included on all email transmittals:

> "This message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and privileged information that is exempt from public disclosure. Any unauthorised review, use, disclosure, or distribution is prohibited. If you received this message in error please contact the sender (by phone or reply electronic mail) and destroy all copies of the original message."

Should information be unintentionally transmitted by a CWA staff member, CWA's IT Department will be made aware of security breach.

Should information be intentionally transmitted by CWA staff member, staff member will be disciplined as outlined in CWA's policies and procedures.

All security incidents will be tracked by CWA's IT Department and will subsequently generate reports as requested by the CEO regardless of transmittal type.

1.1.12 – Encryption

Employees can use encryption software supplied to them by the IT department for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a company computer must provide their Head of Campus with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

1.1.13 – Computer Security and Virus/Adware Protection

Laptop Security

- To provide security against the loss of portable equipment, it is CWA's policy to provide all laptops and notebooks with a "logon password/account" required for the computer to load. The logon password/account will be known only to the IT department and the unit's designated user(s).

Server Security

- Servers are vital to a network, since they provide access to data and resources such as routers and printers. Special measures are needed when a server is accessible over the Internet, since it can then become accessible to users outside the company's intranet.

- It is CWA's policy that all company servers will be placed in a secure location, such as in a locked room with restricted access. In cases when it is not possible to place a server in a locked room, it will be placed in a lockable case, ensuring that the case is always locked.

- It is also CWA's policy to provide additional server and workstation security by a combination of firewalls and anti-virus software.

Virus and Adware Protection

- All servers and workstations property of CWA will have anti-virus and adware removal software installed at all times so that all data input to the system is constantly monitored. IT staff will periodically verify through the product's monitoring tools the virus-free status of each system.

- In addition, daily virus scans will be scheduled to run off hours or at the time the workstation is turned on.

1.1.14 – Violations

Any employee who abuses the privilege of their access to e-mail, Internet or software in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.