Wychwood School
OXFORD

Wychwood, Oxford Cyber Security Policy
Author: JM, AKJ
Inception: May 2018
Date of Next Review: May 2022 or as required

Aim

The aim of this policy is to oversee the cyber security of the network at Wychwood, Oxford and to maintain its integrity from cyber-attack or hacking.

Firewall

Schools and other institutions should protect their Internet connection with a firewall to create a 'buffer zone' between their IT network and other, external networks. Within this buffer zone, incoming traffic can be analysed to find out whether or not it should be allowed onto our network.

At Wychwood School (Oxford) Ltd we have an internet firewall router along with firewalls on each individual PC and Servers. This protects all our devices, particularly those that connect to public or other untrusted Wi-Fi networks.

Security of Settings for your devices and software

Manufacturers often set the default configurations of new software and devices to be as open and multi-functional as possible. Software and devices arrive coming with 'everything on' to make them easily connectable and usable. Unfortunately, these settings can also provide cyber attackers with opportunities to gain unauthorised access to our data, often with ease.

At Wychwood, Oxford the IT manager always checks the settings of new software and devices and, where possible, makes changes which raise the level of security. The IT manager then tests the software and/or devices and, only when they are judged to be secure, are they deployed across the network.

At Wychwood School (Oxford) Ltd we use a server and active directory. Laptops, desktop computers, tablets and smartphones contain data, and they also store the details of the online accounts that you access, so both devices and accounts should always be password-protected.

Each user has a user account and unique password complying with our password policy. The accounts of old employees are disabled and then deleted after a period of six months.

The Wychwood, Oxford network will remember staff and pupils' password history for the last 20 passwords. This means a password that has already been used cannot be repeated within

the next 20 passwords. The maximum password age will be 180 days and the network will require operators to change passwords every 180 days. The minimum password length will be 8 characters with the following complexity requirements: passwords must:

- not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- be at least 8 characters in length
- contain characters from all four of the four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

Extra security

For 'important' accounts, such as banking and IT administration, you should use two-factor authentication, also known as 2FA.

At Wychwood, Oxford two-factor authentication is used for banking, for all contact with the Inland Revenue, Barclaycard and Google and on the mobile telephones of key staff.

Control over access to data and services

To minimise the potential damage that could be done if an account is misused or stolen, staff accounts should have just enough access to software, settings, online services and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them.

Accounts with administrative privileges are only used to perform administrative tasks. This is important because an attacker with unauthorised access to an administrative account can be far more damaging than one accessing a standard user account.

At Wychwood School (Oxford) Ltd we have one administrator and all other users are privileged accounts. All software used is from official sources and is checked by the IT Manager prior to installation. The IT manager is the only person able to install software.

Protection from viruses and other malware

Malware is short for 'malicious software' such as ransomware which makes data or systems it has infected unusable - until the victim makes a payment.

Viruses are another well-known form of malware. These programs are designed to infect legitimate software, passing unnoticed between machines, whenever they can.

There are various ways in which malware can find its way onto a computer. A user may open an infected email attachment, browse a malicious website, or use a removable storage drive, such as a USB memory stick, which is carrying malware.

At Wychwood School (Oxford) Ltd we use Sophos Endpoint Protection and Sophos Intercept X as our malware defence systems

Updating devices and software

It is important that phones, tablets, laptops or computers are kept up to date at all times. This is true for both Operating Systems and installed apps or software. Doing so is quick, easy,

and free. Manufacturers and developers release regular updates which not only add new features, but also fix any security vulnerabilities that have been discovered. Applying these updates or patches is a process known as patching. The IT manager sets the operating systems, programmes, phones and apps to 'automatically update' wherever this is an option. All other updates or patches are applied within a week.

However, all IT has a limited lifespan. When the manufacturer no longer supports your hardware or software and new updates cease to appear, Wychwood, Oxford will consider a modern replacement.

At Wychwood School (Oxford) Ltd we use Windows Update along with Adobe and Java which are all set to check for updates automatically.