IT Security Policy

Contents

Status of this Policy 2
Scope 2
Key Information Assets 2
Physical security 2
Hardware 2
Laptops and Desktops 2
Servers 2
Network equipment 2
Passwords 3
Remote Access 3
BYOD (Bring your own device) 3
Responsibilities of staff 4
Back-up Policy 4
Data Retention Policy 4
Appendix – Approved Software List 5

Introduction

OCN London takes security very seriously. This policy lays out the scope of OCN London's IT security considerations, the means by which OCN London protects those IT security considerations, and the responsibilities of management and staff to uphold these practices.

OCN London holds key information on its stakeholders including centres and, most crucially, learners at those centres. It is therefore imperative that OCN London keeps information as secure as possible and only allows access to staff members where the functioning of the business requires it.

The IT Security Policy is the responsibility of the Head of IT and agreed by the CEO.

The IT Security Policy sits underneath the Data Protection Policy which covers all computerised and non-computerised data security, as well as compliance with GDPR.

The IT Security Policy and Data Protection Policy are enforced by the Security Awareness Policy and supported by the Incidence Response Plan and Incidence Response Reports.

All OCN London policies are informed by the organisations Risk Management Plan and tested and updated at least once a year.

Status of this Policy

This policy does not form part of the formal contract of employment for staff but it is a condition of employment and will abide by the rules and policies made by OCN London from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Scope

The scope of this document applies to any electronic data handled by any OCN London staff member, or consultant hired by OCN London, that relates to the work for OCN London.

Key Information Assets

OCN London's key information assets are grouped as follows:

- Centre information
- Learner information
    - Registration
    - Achievement
    - Assignments
- Qualification and unit information

All key information is stored on the main Quartz database.

Information pertaining to Learner assignments is held on the OPAL and OPT systems.

Physical security

- The premises are accessed with a key and fob system.
- A log must be kept of all keys and fobs in circulation.
- Physical data records must be kept in a locked cabinet on the premises.
- Physical IT equipment must be kept in a locked room.

Hardware

LAPTOPS AND DESKTOPS

- Local firewall on all machines
- AntiVirus on all machines,
- Automatic updates on all machines
- All Operating Systems kept up to date
- Secondary AntiVirus software installed on all machines for secondary ad hoc malware scans

SERVERS

- All on-premise servers non-internet facing and behind Hardware Firewall
- Local Firewall on all machines
- Operating Systems kept up to date.

NETWORK EQUIPMENT

- Hardware Firewall to prevent any outside connections.

- WiFi access points with firmware kept up to date and protected with passwords.

Passwords

OCN London follows the following guidance regarding a successful password policy:

- Maintain an 8-character minimum length requirement (longer isn't necessarily better)
- Don't require character composition requirements. For example, *&(^%$
- Don't require mandatory periodic password resets for user accounts
- Ban common passwords, to keep the most vulnerable passwords out of your system
- Educate your users to not re-use their organization passwords for non-work related purposes
- Enforce registration for multi-factor authentication
- Enable risk-based multi-factor authentication challenges

Office365 and Google password controls follow the above guidance.

In the case of Quartz, passwords expire after 90 days.

Remote Access

Remote access is only allowed by arrangement with IT.

Remote users are required to access with multi-factor authentication. They must set up MFA by adding their own mobile phone numbers as authentication phones and another number (i.e. their office phone) as secondary authentication numbers.

Staff accessing work information, including emails, calendars, Sharepoint, GoogleDrive and OCN London supplied hardware are expected to observe the following policies:

- Always sign out after a session
- Do not save confidential information in folders local to a remote location, e.g. the desktop, usb drives or printed out on paper.
- Do not use laptops or other OCN London supplied hardware on public Wi-Fi connections for example in a café.

BYOD (Bring your own device)

Staff are permitted to use their own devices by prior agreement with IT. Permission will be granted under the following conditions:

- Operating systems are up-to-date and receiving updates from the manufacturer.
- Firewall is switched on and correctly configured.
- Anti-Virus is switched up to date and switched on.
- The device itself must be secured with a strong password and/or biometric data.
- The device may not have software installed that is not either:
    - On the OCN London Approved Software list (see Appendix)
    - A signed application downloaded from an approved App store

Responsibilities of staff

All staff and anyone with an OCN London account will be alerted to their responsibilities regarding security when they are first granted access to OCN London's systems and through regular reminders at staff meetings, appraisals, company wide memos and when any new security risks are discovered.

- Don't open unsolicited attachments
- Exercise common sense for suspicious emails
- Remote PCs - do not install anything without consulting IT.
- No sharing of folder and files with non-OCN London staff without prior consultation with IT. If files in the cloud need to be shared with non-OCN London staff they should be sent as an email attachment.
- Inform management and the Head of IT immediately if they suspect a formerly unidentified data risk or data breach.
- No unencrypted passwords to be saved on non-work devices
- Always sign out after a session
- Do not save confidential information in folders local to the remote machine, e.g. the desktop, usb drives or printed out on paper.
- Secure all non-work devices that are used to access work with passwords.
- Do not use laptops or other OCN London supplied hardware on public Wi-Fi connections for example in a café.

Back-up Policy

The key data assets covered by the back-up policy are:

- Files and folders
- Emails
- Databases
- Websites

OCN London takes a layered approach to back-ups that is tailored depending on the asset being protected. Assets are backed up continually in the location in which they sit to enable easy retrieval. The second layer is an online back-up in a separate cloud based location. These back-ups are taken nightly and kept indefinitely. The third layer is a hard disk back up taken monthly.

Back up methods are detail in the *Detailed Back-up Policy.*

Data Retention Policy

20. OCN London has a duty to retain some staff and learner personal data for a period of time following their departure from OCN London, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example relating to pensions and taxation. Different categories of data will be retained for different periods of time. The exact details of retention periods and purposes are set out in the Records Retention Schedule.

The data protection officer is responsible for implementing and monitoring compliance with this policy. They will undertake an [annual] review of this policy to verify that it is in effective operation.

All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

Hard copy and electronically-held documents and information must be deleted at the end of the retention period.

Hard copy documents and information must be disposed of by shredding.

Retention of data is detailed in the Record Retention Schedule.

Appendix – Approved Software List

The below lists software that is deemed safe to have installed on a device that is or is also used for work purposes.

In the case of users' smartphones on which they have Outlook or Teams installed, OCN London also permits signed applications that have been downloaded from one of the main App stores hosted by Microsoft, Apple or Google.

Software Name	Company	Notes
7Zip		
ABBYY FineReader		
Adobe Acrobat Pro	Adobe	
Adobe Acrobat Reader	Adobe	
Adobe Creative Cloud	Adobe	
Adobe DNG Converter 9.6	Adobe	
Adobe Photoshop Elements	Adobe	
Ansible		
ArchiveSpace	ArchiveSpace	
Audacity		
Audible Manager		
Blackboard Collaborate		
CutePDF		
Drop Box		
EverNote		
Exam View		
Faronics Anti-Virus	Faronics	
Faronics Core	Faronics	
Faronics Data Igloo	Faronics	
Faronics Deep Freeze	Faronics	
Faronics Insight		

FileMaker Pro	FileMaker international	
FileZilla		
Filezilla 3.29		
Firefox		
Foxit PDF		
Gimp		
GIT		
GNUPGP		
Google Chrome		
Google Drive for Desktop		
Google Earth Pro		
Grade Machine		
Grafana		
Grammarly Business		
Graph - Math		
Greenshot		
Hitachi Starboard		
i-learn math toolbox		
Inspiration		
IsadoraCore 2.2.2		
iTunes	Apple	
JAWS		
JING	TechSmith	
Keyboard Pro Deluxe		
Keynote 7.3.1		
Kindle for PC		
Kindle for PC with Accessibility Plugin		
MariaDB		
MathType		
MatLab		
Microsoft Office suite		
Microsoft Teams		
Microsoft Project		
Microsoft Power BI		
Microsoft Visio		
mySQL		
Natural Reader 14		
Notepad++		
OpenNMS		
OpenShot		
Opera 49.0		
Pages 6.3.1		
PaperCut		

PDFArchitect		
PDFCreator, PDFforge		
Power DVD		
Pronunciation Power		
Quartz	Portico	
Quickbooks Pro		
Revit		
Rosetta Stone		
Safari		
SARS		
Screencast-O-Matic		
Skype		
TextWrangler 5.5.2		
VLC 2.2.4		
WinMerge		
WinPlot		
WinRar		
WinSCP		
WinZip		
WireShark		
Wolfram CDF Player		
WS FTP Pro		
XCode		
Xmarin		
XnView		
Zoom Video Conferencing	Zoom.us	
ZoomText		