IT Security Policy

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.
- All machines set up by IT following a set procedure including disabling auto-play, enabling web filtering and removing unnecessary software.
- All devices must lock when the user is not physically present, either by biometric locking or an eight-digit minimum password.

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.
- Access to Firewall settings allowed over the public internet for the Head of IT and UK Cloud Communications only.

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 password controls follow the above guidance.

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

User accounts are audited annually.

When choosing passwords OCN London staff should follow the below guidelines:

- Do not use easily discoverable terms as the basis of passwords, e.g. pet's names, children's names, addresses, etc.
- Do not use the same password for work as you use for personal business.
- A longer password is better, e.g. concatenating three random unrelated words together that is memorable for you but very difficult to guess

In the event of any suspected compromise of a password the password must be changed immediately. Staff should inform IT of the suspected breach and will be assisted in checking the extent of the breach and creating a secure password.

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 save confidential information in folders local to a remote location, e.g. the desktop, usb drives or printed out on paper.

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 that meets the password specifications in the password section and/or biometric data
- The device must be set to lock when the user is not physically present, either by biometric authentication or password inline with the password policy.
- 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, 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

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.

Administrator privileges

Internal administrator accounts are held by the Head of IT and the IT Assistant only. The Head of IT grants admin privileges to the IT Assistant. Both the Head of IT and the IT Assistant are appointed by the CEO. The responsibility for maintaining the security of admin accounts lies with the Head of IT who reports directly to the CEO.

Admin accounts must only be used for admin purposes and not day to day tasks like web browsing or accessing email.

Access granted to outside organisations

OCN London's internet service providers/ network management company UK Cloud Comms has been granted access to the firewall at Angel Gate for the purpose of maintaining the wifi network.

OCN London's Microsoft reseller Hiteishee has access to OCN London's Office 365 tenancy for the purposes of licencing and support.

The suppliers of OCN London's learner management system (Portico Consulting) and finance system (Accounts IQ) have access to the data on those systems.

Client organisations have access to their own data via the QuartzWeb.

Security breaches

If a security breach has been found to occur this will trigger the Data Breach Incidence Response Plan, in which the breach will be identified, contained and prevented from happening again.

Appendix – Approved Software List

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		
AnyDesk		
Audacity		
Audible Manager		
AutoDesk AutoCAD	AutoDesk	
AutoDesk Fusion 360	AutoDesk	
AutoDesk Slicer for Fusion 360	AutoDesk	
Avid Pro Tools		
Beyond Compare 2.X		
Blackboard Collaborate		
CutePDF		
Drop Box		
EosETCnomad Mac Software		
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		
Fitness Trac	Redrock Software Corp.	
FlipBooks 6.6.2		
Fortres Grand Clean Slate		
Fortres Grand Fortres 101		
GeoGebra		
GeoSketchPad		
Gimp		
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		
Kleopatra		
LanSchool		
LifeSize Cloud		
Live Action English		
LucidChart		
MacCaw 1.6.1		
MariaDB		
MathType		
MatLab		
Microsoft Office suite		
Microsoft Project		
Microsoft Visio		
mySQL		
Natural Reader 14		
Notepad++		
OpenNMS		
OpenShot		
Opera 49.0		
Pages 6.3.1		
PaperCut		
PDFArchitect		
PDFCreator, PDFforge		
Power DVD		
Pronunciation Power		
Quickbooks Pro		
Quartz	Portico	
Revit		
Rosetta Stone		
Safari		

SARS		
Screencast-O-Matic		
Skype		
TextWrangler 5.5.2		
VLC 2.2.4		
Wacom Drivers and Utilities		
Weather Link		
WinMerge		
WinPlot		
WinRar		
WinSCP		
WinZip		
WireShark		
Wolfram CDF Player		
WS FTP Pro		
XCode		
Xmarin		
XnView		
Zoom Video Conferencing	Zoom.us	
ZoomText		
Zotero	https://www.zotero.org/	