Information Security Policy

Introduction

1. OCN London takes security very seriously. All staff are made aware of security procedures to be followed in the handling or personal information. Please note that Internet e-mail is never a 100% secure communication medium. By using it you agree that you will send any information by e-mail at your own risk. Whilst OCN London will take all reasonable precautions to ensure that other organisations with whom we deal have good security practices, we are not responsible for the privacy practices of those organisations whose websites may be linked to the site.

Status of this Policy

2. 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

3. In relation to information received from recognised centres, the scope of the policy is restricted to the acquisition, storage, maintenance and sharing of learner data with government agencies.

Key Information Assets

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

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

5. All key information is stored on the main Quartz database.

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

7. All logins for these systems are created and managed by OCN London staff.

Data Security

8. The premises are accessed with a key and fob system.

9. A log must be kept of all keys and fobs in circulation.

10. Physical data records must be kept in a locked cabinet on the premises.

11. Physical IT equipment must be kept in a locked room.

12. Broadband services terminate at a physical firewall device that is correctly configured to control for outside intrusion.

13. Wifi access points must have encrypted transmission and secured with a password.

14. Server access is controlled by the Windows NTLM system.

15. Passwords must be changed every 3 months and meet appropriate strength requirements.

16. Outside connections must be made securely through an encrypted VPN connection.

17. Client access to data is controlled through https sites.

BYOD (bring your own device)

18. OCN London offers staff and guests to the premises at Angel Gate the opportunity to connect to the internet via its wifi service. This is password protected and encrypted.

19. All users of the wifi service agree not to:

- Use the service to access pornographic, violent or other inappropriate material
- Attempt to gain access to or "hack" devices or network items that they have not been granted access.
- Use the service for any other criminal, nefarious or otherwise inappropriate use.

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.*