Oxford Professional Education

Policy Date: December 2020

Reviewed: December 2022

Policy Review Date: December 2024

Reference number 12

Information and Security Policy

Oxford Professional Education (OxPE) Management are committed to providing adequate levels of physical, logical, personal and procedural protection of information and data within its possession.

A process to review the OxPE Information and Security policy every two years is in place.

OxPE has quarterly management meetings where all policies form part of the management agenda to allow clear direction and support from a collaboration of SMT members for security practices.

Information security practices within OxPE have been subject to review by all SMT members and a third-party consultant.

OxPE have a nominated competent individual Director, Tricia Wiley, responsible for information security and privacy issues with regard to the protection of OxPE data.

Security roles and responsibilities are as follows: -

OxPE have in place a process to assess and mitigate the security and business risks posed by engagement with third parties.

All systems and data that is electronically processed is held by 3rd parties who have the required contingency and data recovery processes in place.

Asset Organisation

OxPE have an inventory of all assets where data has been processed, stored or deleted.
If requested by the owner of the data OxPE will provide such inventory to the requester within 2 working days.

OxPE have an **Acceptable Use Policy** that gives clear guidance to employees and contractors as to the acceptable use of information assets and have a mechanism in place for measuring compliance. The internal acceptable use policy shall be made available for review on request.

OxPE have appropriate policies and procedures in place to categorise and label data, and thereby effectively demonstrate the level of protection to be accorded to it. This includes physical and non-physical assets.

Personal Security

OxPE can demonstrate that it has undertaken adequate verification checks on personnel appropriate to their level of access to information and systems throughout the business.

Employees or contractors accessing any data shared with OxPE shall have signed a confidentiality agreement with OxPE and have their legal responsibilities outlined within their contract. A template or form version of such agreement(s) shall be provided upon request within 10 working days.

Measures are in place to train OxPE staff with these minimum-security requirements to the extent that these requirements are applicable to the performance of their functions and duties, and the consequences of any breach of these requirements by them.

OxPE has a documented procedure in place to remove the access rights of individuals upon termination of their employment, engagement or where management deem it necessary. A copy of such procedure shall be provided upon request.

Physical and Environmental

Physical security is in place to protect areas where data is to be processed or stored. The sophistication of controls is appropriate to reflect the identified risks.

OxPE have in place and can evidence adequate processes and procedures for the granting of access to areas where data is to be processed or stored.

OxPE hold quarterly reviews of physical access to areas that store or process data and shall remediate any deficiencies found within a reasonable time and shall, on request, provide with a copy of any remediation report.

All equipment and areas where data is to be processed or stored is physically protected against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.

OxPE can demonstrate an established mechanism for authorising access to equipment and areas where data is to be processed and/or stored, and that a process exists for maintaining the list of authorised personnel.

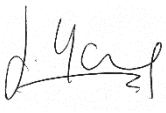
A record of staff and visitors that have accessed the premises shall be maintained. The date and time of such access shall be recorded for all such staff and visitors.

OxPE data relating to third parties will not be transferred off-site without prior written consent, and where this occurs, adequate measures shall be taken to prevent the unauthorised retrieval of OxPE data from media removed from OxPE premises. Adequate measures include measures that relate to the destruction, deletion and overwriting of the information.

Communications and Operations Management

- Changes to facilities and systems that process data must be subject to strict change management control
- Security event logs of systems that contain or process data will be proactively monitored, and the file integrity of the logs shall be preserved. Controls will be implemented to protect logs from unauthorised modification or destruction. Unauthorised changes and unplanned events shall be detected and addressed. **This is covered by our 3rd party**
- Security event logs of systems that contain or process data must be retained for a minimum of 180 days**. This is covered by our 3rd party**
- All email messages coming into and out of OxPE's environment must be scanned for viruses and other malicious code using up-to-date solutions
- Firewalls must be implemented at all internet connections and between any internal network zone. A formal process must exist for the approving and testing of all network connections and changes to the firewall and router configurations
- Intrusion detection systems should be implemented on all systems that store, process or transmit information classified as confidential. Additionally, there should be a process to ensure generated logs are reviewed for suspect activity
- OxPE shall perform vulnerability scans (i) quarterly; and (ii) after any changes are carried out on systems that store and process OxPE data. OxPE shall remediate any deficiencies found within a reasonable time. OxPE shall, on request, provide with copies of any remediation reports
- OxPE shall demonstrate that there are controls in place that address segregation of duties, in order to separate the execution and authorisation of an event
- OxPE shall demonstrate that development and test environments are adequately separated
- Any service delivered by a third party to OxPE shall include agreement of associated security controls, their implementation and monitoring. Any such third party shall have accepted contractual liability for any breach of security
- OxPE shall evidence that appropriate controls are in place to mitigate the threats posed by malicious and mobile code

- OXPEG shall evidence a procedure for back-up and recovery of data that ensures the data will be restored to its original state prior to any event. The procedure shall indicate the person who undertook the process, the data restored and, as appropriate, which data had to be inputted manually in the recovery process
- OxPE shall demonstrate the adequacy of network security controls to protect data within their logical boundary and to ensure that:
    - Only authorised access to information systems and data takes place
    - There is no malicious manipulation of data; and
    - Availability of data is maintained.
- Where any media that has stored data is to be disposed of, reused, or is temporarily transferred from the direct control of OxPE, all necessary measures shall be taken to prevent the unauthorised retrieval of the data, either by over writing (3 times minimum) for disposal and re-use; or adequate encryption for temporary transfer
- Media back-ups of data shall be stored in an offsite facility. Back-ups shall occur on a daily basis
- All back-ups and other media containing data must be physically protected when transported to and from offsite locations
- All printed material containing data must be cross-cut shredded prior to disposal, incinerated or otherwise disposed of, in a manner agreed with any invested third parties in writing, so that it cannot be reconstituted
- OxPE shall ensure that all data is handled in a manner consistent with its sensitivity or 'classification', to include encryption where required
- Where OxPE collects data via a web presence, then it shall sufficiently test, to invested third party requirements, security to ensure the prevention of unauthorised access, or manipulation, of data
- OxPE shall have in place clear policy and guidance on the security and use of email.

Signed: 
Date: December 2022