Data Protection Policy

OPEN's Client's are largely corporate or business entities, but if OPEN does collect, use or store personal data for business purposes then it ensures that :-

- any personal data is processed fairly and lawfully;

- personal data is only processed for specified and lawful purposes;

- OPEN endeavor to hold only relevant and accurate personal data, and where practical, keep it up to date;

- OPEN do not keep personal data for longer than is necessary;

- we keep all personal data secure;

- OPEN endeavours to ensure that any personal data is not transferred to countries outside of the European Economic Area (EEA) without adequate protection.

Data Handling Policy

Aim of Data Handling Policy

- To ensure that approved level of protection shall be used in the transfer of data in relation to its confidentiality.

- To ensure that data is transferred only to named individuals and those who need to know and that data shall be kept to the minimum required.

- To ensure that users have authority from the Client to undertake the transfer of information.

- The contents of this plan are to be distributed to all staff whenever updated. A non-editable signed copy will be stored on our server in a location known by all.

- In the event of any mishandling of data issues, staff are to contact Directors Paul Boland, James Welch, Pol Macdonald or Lynda Thomson.

Safe Haven

The term 'Safe Haven' is used within OPEN to denote either a secure physical location or the agreed set of administrative arrangements that are in place to ensure security classified, personal or other sensitive information is communicated safely and securely.

Safe Havens will be established, where:

- Information can be securely received and transferred.

- Paper-based information is stored securely in lockable containers, as soon as practical.

- All waste potentially containing security classified, personal or other sensitive information is securely retained until it can be securely disposed of or destroyed.

- Conversations discussing security classified, personal or other sensitive information can be held where they cannot be overheard by unauthorised persons.

Digital/Internet Data Transfers

OPEN uses BOX for secure digital transfer and each user within the company has a secure account setup. Where possible data transfers should always be carried out over BOX, however, there may be occasions where data will need to be transferred over other networks. On these occasions the data files must be protected by encryption to protect the data should it fall into the hands of unauthorised persons.

Physical Data Transfers:-

- Physical transfers include paper and portable physical media (USB, hard disks, CDs, DVDs, etc.) In addition to the general principles above physical transfers shall adhere to the following:

- An approved method of transfer shall be determined by discussion with the Client for the type of data being transferred.

- A record of transfers shall be kept under the project folder.

- Portable media shall only be authorised when there is a valid business requirement.

- Only official business approved removable media shall be used.

- Where information is transferred via mail the outer envelope/package shall not be marked with its Security Classification.

- Transfers of data in hard copy form will need to be protected, by using such methods as approved couriers or Royal Mail Track and Trace. Where data is to be transferred by memory stick, CD/DVD or removable hard drive, the media should be encrypted, which will provide adequate protection should it become lost or fall in to the hands of unauthorised persons;
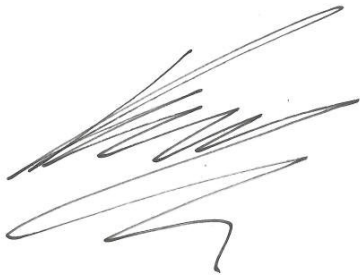
Data Disposal

- Information held on OPEN's systems shall be securely erased in accordance with the businesses Reuse, Disposal and Destruction Policy.

- Information held in paper form shall be securely destroyed in accordance with the business Records Management Policy.

Other Data Handling

- Where there are occasions when new pieces of work require one time only data transfers or data storage, OPEN's staff should request guidance from the Directors.

Signed:

Ben Palmer, Director

February 2019

Record of revisions

Version	Changes from previous version
1	First issue

Version 1