Canning's Data and Information Security Policy

Canning is committed to maintaining the integrity and security of all its data, to complying with all appropriate legislation and to following best practice wherever possible.

To achieve this, all employees and associate trainers must comply with the policies set out below.

Canning also has plans to deal with business continuity and disaster recovery. The IT aspects are dealt with here.

- Private and confidential data: Access is restricted and only permitted to authorised personnel. We are committed to reducing the use of paper records as far as possible, but where we must have them, paper records are kept in a locked cupboard. Access to computer-based data (e.g. Brightpay software for payroll) is password- restricted and limited to authorised personnel.

- Confidential material received from clients in order to help trainers prepare for a course must be deleted from all electronic folders once the course has finished. Any paper copies must also be destroyed.

- The Managing Director occasionally commits all employees to clients' Non-Disclosure Agreements on behalf of the company. These must be rigidly observed.

- IT Systems

  Canning has two physical networks: corporate network and a student network. The student network does not allow access to the corporate network.

  - All users have a password which must not be divulged to anyone else.
  - Access to Canning Database and Xero is restricted to users on a "need to use" basis. Passwords are only issued to employees who need to access these.
  - All users are aware that, when using the internet, the use of inappropriate websites is prohibited.

- Users are aware that any emails containing attachments should be treated with caution. Attachments should only be opened when users are confident that it is safe to do so.
- Canning uses a professional IT support company to maintain its hardware and software. Support is provided via weekly visits and is also available via a 24 hour hotline. Regular reports are supplied to Canning.
- Canning uses anti virus software on all its computers and servers. This updates regularly.
- Canning uses a firewall on the server controlling its corporate network. This is monitored by Canning's I.T. support company.
- Access to the corporate network is restricted to employees of Canning. Associate trainers have access to the "training" network, which contains the material needed to run our courses.
- Canning company data is stored in Microsoft 365 using Microsoft SharePoint Online. Data is stored on multiple SharePoint sites and permissions applied to each site to secure access to company information.
- We have enabled two factor authentication on Xero and Microsoft 365.
- Microsoft SharePoint company data is automatically backed up on a daily basis to a Microsoft Azure UK datacentre.
- IT Support company perform regular checks of hardware to ensure working properly (including test restore).

- Business Continuity
  - Canning's data is hosted by Microsoft 365. The data is stored remotely, and therefore data is accessible from anywhere and uninterrupted by any disruption to Canning's IT systems.
  - The data on Canning's database is all stored remotely, via the database provider, and is accessible via the WWW.
  - Canning's email is hosted by Microsoft 365. The data is stored remotely, and therefore email is accessible from anywhere and uninterrupted by any disruption to Canning's IT systems.
  - This means that Canning's back-office operations could continue virtually uninterrupted in the event of significant disruption to IT systems.

Data Protection

Canning maintains a database which records details of staff, associate trainers, participants and employees of customers and potential customers.

Canning supports and encourages its staff to ensure that the use of this data is consistent with all Data Protection legislation.

- As a Data Controller, Canning has notified the Information Commissioner that it maintains this database. Employees are encouraged to ensure that data is used in accordance with DP legislation. This forms part of any internal database training that Canning runs for its employees.
- Canning complies with GDPR and ensures that all data is held and used legitimately.
- Canning does not share data outside of the organisation. Associate Trainers can only receive vital academic data about participants through the Canning email system, for which they each have an email address and access.
- Any machine which holds Canning’s client or employee data must be password protected and/or encrypted. Where possible the data should not be held locally, and should be accessed remotely.
- All data held or used for marketing purposes must be held and used legitimately, under prevailing legislation. Canning will never use client or participant data to make contact with people who have expressly asked us not to do so. Where possible Canning will offer people the opportunity to manage their own preferences on what marketing materials they receive.
- Canning has a duty of care to participants and clients on its premises, and in pursuit of that duty will sometimes need to collect and hold personal data. This should be destroyed when it is no longer needed; normally when the participant or client has left the premises for the foreseeable future.