

Data Protection Policy

**Introduction**

CANTO Learning Ltd needs to gather and use certain information about individuals in certain cases data will be held to meet legal obligations held towards our stakeholders. This can include students, parents/carers, employees, emergency contacts and stakeholders or other people/organisations that CANTO Learning has a relationship with. This policy describes how the personal data must be collected, handled and stored to meet the company’s data protection standards, and to comply with the law.

**Scope and Rationale**

The primary purpose of the data protection policy is to ensure that CANTO Learning Ltd:

* Complies with data protection law and follows good practice.
* Protects the rights of students, staff and partners.
* Is open about how it stores and processes individuals’ data.
* Protects itself from the risk of a data breach.

It is the policy of the College to ensure that all members are aware of the requirements of data protection legislation in relation to their individual responsibilities.

**Processing Personal Data**

**What constitutes personal data?** Any information related to a natural person or ‘Data Subject’, that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Under GDPR Law CANTO Learning Ltd is obliged to ensure that all data shall:

1. **be processed fairly and lawfully;**
2. **be held only for specified purposes and not used or disclosed in any way incompatible with those purposes;**
3. **be adequate, relevant and not excessive;**
4. **be accurate and kept up-to-date;**
5. **not be kept for longer than necessary for the particular purpose;**
6. **be processed in accordance with data subjects’ rights;**
7. **be kept secure;**
8. **not be transferred outside the European Economic Area unless the recipient country ensures an adequate level of protection.**

These rules apply whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. Processing of data includes any activity that involves the handling of data including its, collection, use, storage, adaption, dissemination or disposal.

In view of the recent global pandemic it should be recognised that although medical information is considered sensitive, under GDPR article 9 there is provision for this information to be shared without consent should it be deemed of public interest. However consideration will always be given to data security and this will be applied on an individual case basis. Under this guidance CANTO has the right to request information regarding travel and socialisation to safe guard the college community

Any processing of such information must be done in accordance with the principles outlined above. To comply with the first principle (fair and lawful processing), at least one of the following conditions must be met:

**The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:**

**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

**(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

**(d) Vital interests:** the processing is necessary to protect someone’s life.

**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

In all instances where consent is needed this will be requested in an easily accessible form, with the purpose for data processing attached to that consent - meaning it must be unambiguous. Consent must be clear, using clear and plain language. It must be as easy to withdraw consent as it is to give it.​  Explicit consent is required only for processing sensitive personal data - in this context, nothing short of “opt in” will suffice. However, for non-sensitive data, “unambiguous” consent will suffice see Article 7 and in Recital 42 where the GDPR states that “where processing is based on the data subject’s consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.”).

**Data Security**

CANTO Learning Ltd takes the data security seriously and to reduce the risk of a data breach and has undertaken several technical measures. This includes email and other forms of encryption. Our 3rd party IT company support CANTO in this process maintaining and monitoring our server and cloud for possible breaches. Data stored on paper will be held within locked rooms and shredded when no longer needed. Privacy Impact Assessments will monitor along with regular checks on data by the quality assurance team. Staff are kept informed of CANTO’s data protection policy and training is provided when appropriate.

All staff are aware that appropriate permissions are needed for personal data and that this must be kept securely at all times whether in paper or electronic format.

No personal data should be passed on orally to a third party to an unauthorised third party with out the express consent of the data subject.

**Responsibilities**

All staff or other individuals who have access to, or who use, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised person.

CANTO Learning Ltd will take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data. All staff and members should be aware that guidelines and regulations relating to the security of manual filing systems and the preservation of secure passwords for access to relevant data held on computer should be strictly observed.

Personal data about an individual must not be placed on the world wide web unless the individual whose data is used has given his or her express consent.

Any failure to comply with the provisions of the GDPR could result in reputational and financial costs to the College. All staff must therefore familiarise themselves with the general aspects of GDPR.

Any data protection concerns should be addressed to the senior leadership team in the first instance.

**Bring your own device**

In line with CANTO Learning’s Bring Your Own Device policy the college recognises the benefits that using a personal device can bring whether they be laptop, smart phone or tablet. However it is recognised that the college must remain in control of it’s data and that this must fully comply with the GDPR legislation.

To ensure that this is the case before using a personal device staff are expected to sign to agree to the terms of the BYOD policy. The BYOD policy is designed to comply with all aspects of the GDPR legislation.

**Photographs within the college**

To ensure that CANTO meets high standards for data protection it will request specific consent when using individual’s pictures for varying data processing reasons. Due to the variety of processing reasons these need to be considered separately and some are outlined below, it should be noted that these are not exclusive to the college but in all cases specific consent will be requested and clear guidelines given as to the use and length of time these will be maintained for.

**Photographs within the college**

Photographs used in the identity management can be essential as part of an individuals programme, however once an individual leaves the college this should be deleted as it is no longer needed for the purpose for which it was held.

Photographs used in displays within the building will require consent from the individual for this purpose, on giving consent it will be agreed that no picture will be displayed for longer than 6 months. Once the individual leaves the college pictures on display will be removed unless additional consent has been obtained. This additional consent maybe particularly relevant should this picture form part of a larger display. If additional consent is sort this should be for no longer than an additional period of 6 months.

Photographs to be used on the website/facebook or other social media platforms must have explicit consent from the individual for a period of 12 months. Regular checks are to take place of these sites to ensure that appropriate consent is obtained for all individuals featuring. When a student leaves additional consent may be obtained to allow a particular picture or pictures to feature, the consent in this case must be specific and monitored.

Photographs to be used in promotional material will have explicit consent from the individual.

This consent will state that images will be maintained on the promotional material for a period of up to 12 months. Regular checks are to take place of the material to ensure that appropriate consent is obtained for all individuals featuring. When a student leaves additional consent may be obtained to allow particular picture to feature, consent in this case must be specific and monitored.

Photographs to be used in promotional material such as banners etc will have explicit consent from the individual. Due to costs involved in the creation of such promotional materials it is recognised for this that these materials would need to be kept for a longer period of time. When seeking consent from individuals for this purpose clear guidance will be given as to the use and the length of time the consent is required for before permission is requested.

**Privacy by design**

CANTO Learning Ltd undertakes an approach to activities within the organisation that incorporates privacy and data protection compliance from the start. To comply with Article 25 of GDPR the college ensures that appropriate organisational and technical measures are in place to support the handling of data. To ensure that privacy by design is embedded within the organisation Data Privacy Impact Assessments are implemented to support this process.

**Data Privacy Impact Assessments (DPIA’s)**

To ensure that CANTO complies with Article 35 DPIA’s will be carried out when it is assessed that a processing activity may take place that could place a high risk on data. As part of this the college will ensure that the DPIA is in place early in the life of a new processing activity so that risks can be assessed and recommendations made and implemented. A CANTO Learning DPIA will seek to

* 1. Identify the need for a DPIA.
* 2. Describe the information flow.
* 3. Identify data protection and related risks.
* 4. Identify data protection solutions to reduce or eliminate the risks.
* 5. Sign off the outcomes of the DPIA.
* 6. Integrate data protection solutions into the processing activity.

**Right to be forgotten/Right to erasure**

Under Article 17 of GDPR individuals have a right to have personal data erased. This is also known as the ‘right to be forgotten’ and is newly implemented. The right only is not absolute and only applies in certain circumstances.

The college will apply the right to erasure if:

* the personal data is no longer necessary for the purpose which you originally collected or processed it for;
* The consent given which provides our lawful basis for holding the data, is withdrawn; (should be noted that in certain cases this information maybe considered a vital interest for the individual and therefore provide a basis for data to be retained)
* we are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
* we are processing the personal data for direct marketing purposes and the individual objects to that processing;
* we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
* we have to do it to comply with a legal obligation; or
* we have processed the personal data to offer information society services to a child.

**The right to erasure does not apply if processing is necessary for one of the following reasons:**

* to exercise the right of freedom of expression and information;
* to comply with a legal obligation;
* for the performance of a task carried out in the public interest or in the exercise of official authority;
* for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
* for the establishment, exercise or defence of legal claims.

### Do we have to tell other organisations about the erasure of personal data?

CANTO will endeavour to contact each recipient of the data and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked CANTO will individuals about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency, or other body to which the personal data are disclosed.

**Right to portability**

GDPR gives the individual the right to ask for their data in a commonly used format, the individual may also request that this data is transmitted directly to another controller. This right only applies to personal data and data that in the first instance has been provided to the college. When the college receives a request for data to be passed on in this way it will ensure that it is: structured; commonly used; and machine-readable.

**Subject access requests**

A Subject Access Request is a request for personal information that is held by the college about an individual. If an individual wishes to exercise their subject access right, the request must be made in writing to the college. The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of processing of their personal data. Under the GDPR and the current Data Protection Act (DPA), individuals have the right to obtain confirmation as to whether personal data is being processed. This request will be responded to within a period of 30 days.

An individual may apply request the following information from the college if personal information is being processed: the reasons why their data is being processed;

* the description of the personal data concerning them;
* anyone who has received or will receive their personal data; and
* details of the origin of their data if it was not collected from them.

To ensure that CANTO Learning fully complies with GDPR no charge will be made for this service unless as per GDPR the request is *‘manifestly unfounded or excessive’*. Should this be the case the college may request a reasonable fee for this service.

The college also retains the right under GDPR to withhold personal data under GDPR should disclosing it *‘adversely affect the rights and freedoms of others.*

All Subject Access Request should be made in the first instance to a member of the SLT.

**CCTV**

To maintain the security of the college and site CANTO instructs a third party to maintain a CCTV system on its behalf. To ensure that this system is as un-intrusive as possible this system operates only outside of normal operating hours. The system is designed so that it will not provide facial recognition but is used to identify and deter criminal activity. Our third party maintain this system in line with their GDPR policy and procedures. As per their policies images captured will be stored for 30 days unless specified by CANTO Learning and in the case of criminal activity will be stored for 60 days. Should a need a rise to share images with authorities these will be done securely. As per our operators policy all images and alerts are destroyed/deleted after a period of 60 days.

**Biometrics**

As an organisation we use biometrics to assist us in monitoring both staff and student attendance, as part of this process we comply with the requirements of the Protection of Freedom Act 2012 as do Live Register who maintain this system on our behalf. As part of this process we ensure that permissions are requested before any biometric data is taken. An alternative form of registration is offered should any individual object to the taking of biometric data.

If a person withdraws consent after first giving it we will ensure that any biometric data is deleted. Regular checks are undertaken to ensure that the Biometric data base is maintained in line with current permissions.

**Breach Notification**

CANTO Learning Ltd recognises that in the event of a data breach certain actions must take place. Should a data breach occur as in the case of a loss, theft, unauthorised access etc actions followed must meet GDPR standards. Critical to this is the reporting of the breach to supervisory authority (ICO) within 72 hours. If it is assessed that the breach is such that it places the data subject at a high privacy risk the individual should be informed of the breach within the same period.

Updated H.Dear 19th June 2019

Updated H.Dear April 2020