ACCOUNTING TECHNICIANS IRELAND

DATA PROTECTION POLICY

GENERAL DATA PROTECTION REGULATION

Document Control

Owner: Data Protection Officer

Distribution List: Relevant individuals who access, use, store or otherwise process Personal Data on behalf of Accounting Technicians Ireland

VERSION NUMBER	DATE	DETAILS OF REVISIONS
1.0	21/12/2017	

1. Introduction

This Policy sets out the obligations of The Accounting Technicians Ireland ("the Company") regarding data protection and the rights of students, members, service providers (contractors/sole traders) and business contacts ("data subjects"). This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the General Data Protection Regulation (GDPR) which replaced the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003), (the Acts), as and from 25th May 2018.

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, and identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

2. Scope

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company's employees, agents, contractors or other parties working on behalf of the Company.

The policy covers both personal and sensitive personal data held in relation to data subjects by the Company and applies equally to personal data held in manual and automated form.

All personal and sensitive personal data will be equally referred-to as personal data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated:

- Subject Access Request procedure
- The Data Retention and Destruction Schedule
- Procedures for Engaging Data Processors
- The Data Security Breach Notification procedure
- Data Security Policy
- Data Incident Log
- Awareness staff training records

3. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. Article 5 in the GDPR states that all personal data must be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes subject to appropriate safeguards, and provided that there is no risk of breaching the privacy of the data subject.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed is erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
g) Article 5(2) states that the Controller is responsible for and must be able to demonstrate compliance with the Data Protection Principles.

3.a. Lawful, Fair and Transparent Data Processing

1) The Regulation seeks to ensure that personal data is processed lawfully, fairly and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The Company will ensure that at least one of the conditions outlined above will be satisfied whenever any processing activities take place.

2) In order to obtain personal data fairly and in a transparent manner, The Company will make the data subject aware of the following at the time the data is collected directly:

- Identity of the controller and the data protection officer (or equivalent)
- Purpose and legal basis for processing. An explanation of the legitimate interest of the Company will be provided if it is being used as the legal basis.
- Data subject's rights to withdraw consent, request access, rectification or restriction of processing.
- Data subject's rights to complain to the Data Protection Commissioner's Office
- Recipients of the personal data.
- Storage periods or criteria used to determine the length of storage.
- Legal basis for intended international transfer of data to a third country or organisation, including the fact that either the receiving country has an adequacy decision from the Commissioner or other appropriate safeguards are in place and how to obtain a copy.

In situations where the data is not being collected directly from the data subject, the Company will provide the source along with the other information listed above to the data subject within a reasonable period after obtaining the data but not more than one month. Information will not be provided to the data subject if it will require disproportionate effort or it would render it impossible or seriously impair the purpose of the data processing.

The Company will place a Fair Processing Notice in a highly visible position, if it intends to record activity on CCTV or video.

The Data Subject's data will not be disclosed to a third party other than to a party contracted to the Company and operating on its behalf.

3.b. Processed for Specified, Explicit and Legitimate Purposes

The Company follows this purpose limitation principle and only collects and processes personal data for the specific purposes set out in the "Record of Processing Activities" document held by the Company, see 3.g. below. The purposes for which we process personal data will be informed to data subjects at the time their personal data is collected or not more than a month if obtained from a third party.

The Company will not further process personal data in a manner that is incompatible with those purposes unless:

- the consent of the data subject has been obtained, or
- if the further processing is for archiving purposes in the public interest or scientific and historical research or statistical purposes and the appropriate safeguards are in place and there is no risk of breaching the privacy of the data subject.

3.c. Adequate, Relevant and Limited Data Processing

The Company follows this data minimisation principle and only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects.

3.d. Accuracy of Data and Keeping Data Up to Date

The Company will ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data will be checked when it is collected and thereafter, see below. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

- Remind employees, students and members on an annual basis to inform the Company of any changes to their details
- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date.
- Conduct annual audit to establish the need to keep certain Personal Data.

- Send out an annual mailshot to all individuals on the Companies databases to ensure that consent is requested for further marketing etc
- Amend inaccurate data which has been notified to the Company by the Data Subject or is revealed as a result of a subject access request.

3.e. Timely Processing

The Company follows this storage limitation principle and does not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed.

The Company will verify whether statutory data retention periods exist in relation to the type of processing e.g., personal data may need to be kept in order to comply with tax, health and safety, or employment regulations etc. If the law is silent, internal data retention periods will be set to meet the storage limitation principle.

Retention periods will be set considering the purpose or purpose for which the data is collected and used, and once the storage periods expire, data will be securely deleted/destroyed in the absence of a sound new lawful basis to retain it. However, personal data may be stored for longer periods by the Company insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific, historical research or statistical purposes ensuring appropriate safeguards are in place i.e. irreversibly anonymised.

The Company has a Data Retention & Destruction Schedule, review for further details

3.f. Secure Processing

The Company will ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. The state of technological development, the cost of implementing the measures, the nature of the data concerned and the degree of harm that might result from unauthorised or unlawful processing are all taken into account when the Company are determining the security measures that are put in place. Further details are outlined in the Company's Security Policy

3.g. Accountability

Under the GDPR, organisations are obliged to demonstrate that their processing activities are compliant with the Data Protection Principles. The principle of accountability seeks to guarantee the enforcement of the Principles.

The Company will demonstrate compliance in the following ways:

- By keeping an internal record of all personal data collected, held or processed as per Article 30 - "Records of Processing Activities". Upon request, these records will be disclosed to the Data Protection Commissioner's Office.

  When the Company is acting as a Data Controller this record will contain the following:
  - Contact details of the Controller/representative/Data Protection Officer
  - List of personal data being processed
  - Categories of data subjects
  - Processing activities
  - Categories of recipients with whom the data will be shared
  - Retention periods
  - Deletion methods
  - International transfers and measures in place to ensure they are lawful

- Detailed descriptions of the security measures implemented in respect of the processed data

When the Company is acting as a Data Processor this record will contain the following:

- Name of Controller
- Name of Data Protection Officer
- Categories of processing carried out on behalf of the Controller
- International transfers and measures in place to ensure they are lawful

- In order to assess the potential risks arising out of any new processing activity the GDPR requires organisations to conduct a Data Protection Impact Assessment (DPIA). The Company will demonstrate its compliance by carrying out Assessments whenever any new processing activity is proposed, especially where it involves new technologies, resulting in a high degree of risk for data subjects. After the PIA has been carried out and if all the risks can not be mitigated, then the Company will consult with the Office of the Data Protection Commissioner. The DPIA will be overseen by the Company's Data Protection Officer and the DPIA's will be filed and retained as proof of compliance.

- The Company will appoint a Data Protection Officer if required i.e. if its core data processing activities involve:
  - Regular and systematic monitoring of data subjects on a large scale; or
  - Processing sensitive personal data on a large scale.

- The Company maintains a data protection document framework i.e. policies & procedures, training records etc.

- The Company ensures that data protection by design is addressed throughout the life cycle of any processing activity but especially at the time of planning the means and type of processing and during the processing itself. Necessary safeguards are integrated into the Company's systems with the use of data minimisation and pseudonymisation as privacy enhancing tools. The Company assess the risks of a process and tries to mitigate those risks in order to meet the data protection by design requirements.

  The Company also ensures that data protection by default is implemented by choosing the most data protective setting as the default i.e. users will have to opt in to any settings that presents greater risks. By default, only the personal data that is necessary is processed.

4. The Rights of Data Subjects

The Company has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the Regulation.
As part of the day-to-day operation of the organisation, the Company's staff members engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by the Company, such a request gives rise to access rights in favour of the Data Subject, the Regulation sets out the following rights applicable to data subjects:

- The right to be informed (see section 3.a(2) above);
- The right of access;
- The right of rectification;
- The right to erasure (also known as the "right to be forgotten");

- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights with respect to automated decision-making and profiling.
- The right to withdraw consent

The Company's staff members will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible.

The Company has a Data Access Request Policy/Procedure, refer to this document for detailed information on the topic.

5. Transferring Personal Data to a Country Outside the EEA

The Company may from time to time transfer ("transfer" includes making available remotely) personal data to countries outside the Economic European Area (EEA).

The transfer of personal data to a "third country" i.e. outside the EEA, will only take place if one or more of the following applies:

- Is a country that the European Commission has determined to have an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority; certification under an approved certification mechanism as provided for in the Regulation; contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subjects or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under Irish or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

6. Data Breach Notification

The Company have outlined the procedure for data breach notification in a separate document, see Data Breach Procedure for Management (detailed procedure covering notification to the Office of the Data Protection Commissioner) or for Staff (detailed procedure outlined up to the point where Management are notified of the breach) along with an incident log and form. See the relevant document for more details.

It should be noted that the Company treat data breaches very seriously and any employee who becomes aware of a likely data breach and fails to notify the Data Protection Officer or a member of

the Data Protection Committee may be subject to the Companies disciplinary procedure depending on the severity of the breach.

7. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data:
  - Will be appropriately trained to do so;
  - Must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation
  - Bound to do so in accordance with the principles of the Regulation and this Policy by contract
- All employees, agents, contractors, or other parties working on behalf of the Company:
  - Will be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy and will be provided with an opportunity to read this Policy. A document stating that this document has been read and understood should be signed by all relevant parties.
  - That need access to and use of, personal data in order to carry out their assigned duties correctly will have access to personal data held by the Company.
- Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

8. Implementation

The Company ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Regulations. See the Company's procedure on Engaging Third Party Processors for further details.

Failure of a Data Processor to manage the Company's data in a compliant manner will be viewed as a breach of contract.

Failure of the Company's staff members to process Personal Data in compliance with this policy may result in disciplinary proceedings.

9. Data Protection Officer

XXXXXXXX acts as the Data Protection Officer & his/her contact details are **XXXXXXXX.**

XXXXXXXX acts as the Data Protection Committee, and their contact details are:

10. Policy Has Been Approved

This Policy will be reviewed and updated on an annual basis, or sooner if required.

This Policy has been approved and authorised by:

NAME: _____

POSITION: _____

DATE: _____

SIGNATURE: _____

APPENDIX 1

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Pseudonymous Data	This data is still treated as personal data because it enables the identification of individuals albeit via a key.
Anonymous Data	This data Is rendered anonymous because there is no way that an individual can be identified from this data. Therefore, the GDPR does not apply to such data.
Personal Data	Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by the Company to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.