# ATE Data Protection Policy

Date: May 2018
Review date: May 2021
Approved by Board of Trustees: November 2019

## 1. Context and overview

### Introduction

ATE needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, , employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

### Why this policy exists

This data protection policy ensures ATE:

- Complies with General Data Protection Regulations 2018 and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

### General data Protection Regulations

The General Data Protection Regulations 2018 (GDPR)came into effect on 25th May 2018 replacing the Data Protection Act of 1998. The GDPR applies to 'personal data' meaning any information relating to any person who can be directly (or indirectly, from information contained in the data) identified.

Details of the GDPR can be found in Appendix A

## 2. People, risks and responsibilities

### Policy scope

This policy applies to:

- The ATE office
- All places where ATE is delivering
- All staff and volunteers of ATE working remotely
- All contractors, suppliers and other people working on behalf of ATE

It applies to all data that the company holds relating to identifiable individuals. This includes:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- All other information relating to individuals

## Data protection risks

This policy helps to protect ATE from real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

## Responsibilities

Everyone who works for or with ATE has responsibility for ensuring data is collected, stored and handled appropriately.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

These people have key areas of responsibility:

- The Board of Trustees is ultimately responsible for ensuring that ATE meets its legal obligations.
- The Data Protection Officer (currently the Operations Director) is responsible for:
    - Keeping the Board of Trustees updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging any appropriate training and advice necessary for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data ATE holds about them (also called ‘subject access requests’).
    - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

## General staff guidelines

- The only people able to access data covered by this policy must be those who need it for their work.
- Children's data must not be shared informally, i.e. where the sharing of a child's personal information is not in that child's best interests.
- Staff and volunteer information must only be shared on a need to know basis. When access to confidential information is required, staff can request it from the data protection officer.
- Where necessary, ATE will provide training to employees to help them understand their responsibilities when handling data.
- Employees must keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used and they must never be shared.
- Personal data must not be disclosed to unauthorised people, either within the company or externally.
- Data must be regularly reviewed and updated if it is found to be out of date. If no longer required, it must be deleted and disposed of.
- Volunteers and employees must request help from the Operations Director or the Data Protection Officer if they are unsure about any aspect of data protection.

## Data storage

These rules describe how and where data must be safely stored. Questions about storing data safely must be directed to the Data Protection Officer.

When data is stored on paper, it must be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out:

- When not required, the paper or files must be kept in a locked drawer or filing cabinet.
- Employees must make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts must be put in the confidential waste or shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data must be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a memory stick, CD or DVD), these must be encrypted and/or kept locked away securely when not being used.
- Data must only be stored on designated drives and servers and must only be uploaded to a secure cloud computing service.
- Servers containing personal data must be sited in a secure location, away from general office space.
- Data must be backed up frequently. Those backups must be tested regularly, in line with the company's standard backup procedures.
- **Data must never be saved directly to laptops or other mobile devices like tablets or smart phones**.
- All servers and computers containing data must be protected by approved security software and a firewall.

## Data use

Personal data is of no value to ATE unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees must ensure the screens of their computers are always locked when left unattended.
- Personal data must not be shared informally. In particular, it must never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data must never be transferred outside of the European Economic Area.
- Employees must not save copies of personal data to their own computers.

## Data accuracy

The law requires ATE to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort ATE must put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff must not create any unnecessary additional data sets.
- Staff must take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- ATE will make it easy for data subjects to update the information ATE holds about them.
- Data must be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it must be removed from the database.

## Subject access requests

All individuals whose personal data is held by ATE are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests can be made verbally or in writing (including email) to ATE. ATE will always verify the identity of anyone making a request before supplying any information. ATE aims to provide the relevant data within 14 days, but in any case will provide it within one month.

## Disclosing data for other reasons

In certain circumstances, the GDPR allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ATE will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Board of Trustees and seeking legal advice where necessary.

## Providing information

ATE aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a Privacy Policy, setting out how data relating to individuals is used by the company.

# Appendix A

# General Data Protection Regulations

## Data Protection Law

The General Data Protection Regulations 2018 (GDPR)came into effect on 25th May 2018 replacing the Data Protection Act of 1998. The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

The GDPR requires that personal data shall be:

- collected and used fairly, stored safely and not disclosed unlawfully;
- processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 GDPR in order to safeguard the rights and freedoms of individuals;
- 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.
- the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

**The GDPR provides the following rights for individuals:**

The right to be informed

The right of access

The right to rectification

The right to erasure

The right to restrict processing

The right to data portability

The right to object

Rights in relation to automated decision making and profiling.

**The Right to be informed**

- ATE must provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.
- ATE must provide privacy information to individuals at the time we collect their personal data from them.
- if we obtain personal data from other sources, ATE must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when ATE do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information ATE provides to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.
- User testing is a good way to get feedback on how effective the delivery of your privacy information is.
- ATE must regularly review and, where necessary, update its privacy information. ATE must bring any new uses of an individual's personal data to their attention before we start the processing.
- Getting the right to be informed correct can help us to comply with other aspects of the GDPR and build trust with people but getting it wrong can leave us open to fines and lead to reputational damage.

**The Right of Access**

- Individuals have the right to access their personal data.

- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- ATE has one month to respond to a request.
- ATE cannot charge a fee to deal with a request in most circumstances.

**The Right to Rectification**

- The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- ATE has one month to respond to a request.
- In certain circumstances ATE can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

**The Right to Erasure**

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- ATE has one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on ATE to consider whether to delete personal data.

**The right to restrict processing**

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, ATE are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- ATE has one month to respond to a request.
- This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

**The Right to Data Portability**

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.
- Some organisations in the UK already offer data portability through midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

**The Right to Object**

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies ATE may be able to continue processing if we can show that we have a compelling reason for doing so.
- ATE must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- You have one month to respond to an objection.

**Rights in relation to Automated Decision Making and Profiling.**

- The GDPR has provisions on:
    - automated individual decision-making (making a decision solely by automated means without any human involvement); and
    - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
- The GDPR applies to all automated individual decision-making and profiling.