General Data Protection Regulation UK Policy

The wording in this policy reflects the requirements of the Data Protection Act 2018. See law relating to this documents below for more information.

Data Protection Act 2018:

www.gov.uk/data-protection-act-2018

Guide to General Data Protection Regulations 2018 (Information Commissioners Office ICO):

ico.org.ukguide-to-the-general-data-protection-regulation-gdpr/

Introduction

Purpose

AACC is committed to protecting the privacy and security of your personal information and to being transparent about how it collects, stores and uses the personal data about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

AACC has appointed a data protection officer. Their role is to inform and advise the organisation on its data protection obligations. They can be contacted at abingtonannexefinance@gmail.com . Questions about this policy, or requests for further information, should be directed to the data protection officer.

Definitions

"Personal data or personal information" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

AACC will comply with data protection law. We will do this by:

- Processing and storing personal data lawfully, fairly and in a transparent manner.
- Collecting personal data only for specified, explicit and legitimate purposes.
- Processing and storing personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keeping accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Storing personal data only for the period necessary for processing.
- Adopting appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- Telingl individuals the reasons for processing and storing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where AACC processes and stores special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with guidelines from the Information Commissioners Office (ICO) on special categories of data and criminal records data.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies (where applicable) or other background check agencies.

We will collect additional personal information during job-related activities throughout the period of you working for us.

Criminal Offence Data

For further details on processing Criminal Offence Data please follow the link below to the Information Commissioners Office (ICO).

ico.org.uk/criminal-offence-data

“At a glance

- *To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.*

- *The Data Protection Bill deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.*
- *You can also process this type of data if you have official authority to do so because you are processing the data in an official capacity.*
- *You cannot keep a comprehensive register of criminal convictions unless you do so in an official capacity.*
- *You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this."*

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities.

- We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you during you working for us.

AACC will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment for a worker, contractor or volunteer relationship, apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems.

The setting keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process

it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

The setting will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless he/she agrees otherwise.

If the individual wants additional copies, the setting will charge a fee of £5.00 which will be based on the administrative cost to the setting of providing the additional copies.

To make a subject access request, the individual should send the request to abingtonannexefinance@gmail.com. In some cases, the setting may need to ask for proof of identification before the request can be processed. The setting will inform the individual if it needs to verify his/her identity and the documents it requires.

The setting will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the setting processes large amounts of the individual's data, it may respond within three months of the date the request is received. The setting will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the setting is not obliged to comply with it. Alternatively, the setting can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the setting has already responded. If an individual submits a request that is unfounded or excessive, the setting will notify him/her that this is the case and whether or not it will respond to it.

Data security

AACC takes the security of HR-related personal data seriously. The setting has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Staff sign a confidentiality agreement on induction that takes into consideration the use of relevant personal data as well as the due process of dealing with Children's Records.

Please see our **Confidentiality and Client Access to Records Policy**, **Provider Records Policy** and our **Information Sharing Policy**.

Staff who have access to personal data regarding staff members and volunteers in the setting ensure that the data is stored securely and that it is only shared with the relevant suppliers, i.e. payroll processors.

All staff ensure that any paper documents containing personal data are stored securely.

All staff ensure that any electronic documents are stored with a secure provider, additionally making sure relevant documents are 'locked'.

When sending electronic documents all staff ensure that they are sending the information to the correct recipient.

Where the setting engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Taking Photos in Schools:

The following information is taken from the Independent Commissioners Office (ICO)

Your data matters/schools/photos ICO.org

"Taking photos in schools

Does the Data Protection Act stop me taking photos of my children at school?
The Data Protection Act is unlikely to apply in most cases where photographs or videos are taken in schools and other educational institutions.
If photos are taken for personal use they are not covered by the Act.
Photos taken for official school use may be covered by the Act, so pupils and students should be advised why they are being taken.
Examples
Personal use:
A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.
Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.
Official use:
Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.

A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.
Media use:
A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act."

Impact assessments

Some of the processing that the setting carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the setting will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If the setting discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The setting will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

We follow the guidance on Data Breach Procedures from the Information Commissioners Office. For further information, please click the link below.

https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/

International data transfers

HR-related personal data may be transferred to countries outside the EEA to fulfil our contract with members of staff. If data is transferred outside the EEA it will be on the basis of legal Safeguarding and Child Protection Requests or to fulfil our contract regarding staff employment with us. We ensure that all third parties comply with GDPR.

Individual responsibilities

Individuals are responsible for helping the setting keep their personal data up to date. Individuals should let the setting know if data provided to the setting changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the setting relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the setting) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the setting's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Corporate email

Email is an essential part of work at AACC. If staff have access to the AACC email they should use it for work only.

- **Work-related use** - use of corporate email for work-related purposes without limitations. For example, signing up for newsletters and online services that will help in job or professional growth.
- **Personal use** – the management committee do not allow the AACC email address to be used for any personal use. This protects our equipment and files from possible viruses.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the setting's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests

under this policy, will receive additional training to help them understand their duties and how to comply with them.

Rights of the Child:
The management committee hold with the highest regard the rights of the children within our setting. The management committee and staff are all aware of the articles on the rights of the child published by Unicef. The following articles are related to this policy.
UNICEF Rights of the Child

Monitoring and Review:

This policy will be monitored by the administrator and the manager of AACC will be reviewed at least annually.

Risk Assessments:

Risk assessments will be carried out regularly by the trustees of the committee and the staff and management of AACC.

Data Protection:
The setting's record keeping systems meet legal requirements; means of storing and sharing that information take place within the framework of the Data Protection Act 2018 and the Human Rights Act 1998.

ADOPTION AND ANNUAL REVIEW OF THE POLICY

This policy was adopted at a meeting of: **Abington Out of School Club**.

Print Name: RUTH BEACH
Date: 18/07/2018
Role: ADMINISTRATOR

This policy was reviewed on:	Signature and name:	This policy was amended on:	Signature and name:
13/11/2018	R BEACH	13/11/2018	R BEACH
27/01/2020	R BEACH	27/01/2020	R BEACH
22/11/2021	R Beach		
10/11/2022	E Turner	10/11/2022	E Turner