

✓ updated on
one drive

[illegible]



Please also refer to the policy 2.5 Record Keeping and Document 16.1 Data Register.

Statement of intent

Aiming Higher recognises the right of all data subjects to the protection of their personal data and accepts that personal details belong to each individual. Appropriate systems are in place to ensure that such personal information that we collect in the course of our work is kept safe and secure at all times.

We are fully compliant, in our responsibilities with regard to Data Protection legislation in accordance with the Data Protection Act 2018 and with GDPR. This Act makes provision about the processing of personal data. Most processing of personal data is subject to the GDPR.

Definitions of Acronyms, Jargon, or Terms

Term	Refers to:
Workforce	All staff contracted to work for and paid by Aiming Higher
Volunteers and Students	Any individual carrying out Aiming Higher's duties as a volunteer or through a school, college, university or Job Centre work experience scheme
Service user	Any individual in receipt of Aiming Higher services or taking part in its projects and activities
Data subjects	Individuals whose data is held, in hard copy or electronic form, by Aiming Higher
Contractors	Any individual(s) and/or company paid to carry out work on behalf of Aiming Higher
DPA	Data Protection Act 1998
GDPR	General Data Protection Regulations 2018
Data Protection Officer (DPO)	The GDPR introduced a duty for organisations to appoint a Data Protection Officer (DPO) if they are a public authority or body, or if they carry out certain types of processing activities. DPOs assist in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level and can be an existing employee or externally appointed. DPOs can help us

Page 2 of 11

231-233 Church Street, Blackpool FY1 3PB Telephone: 01253 206448

Email: info@aiminghighercharity.org.uk Reg Charity: 1144664



demonstrate compliance and are part of the enhanced focus on accountability.

The Data Controller	means a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be, processed
The Data Processor	The data processor is responsible for control of data and may get another organisation to be their data processor ie to process the data on their behalf. Data processors are not subject to the Data Protection Act. The responsibility of what, and how, it is processed remains with Aiming Higher as the Data Controller. There should be a written contract with the data processor who must have appropriate security provisions in place.
Personal Data	Data relating to a living person who can be identified from the data, or other information held by the data controller.

Scope

This policy applies to all employees, volunteers and students or any individual or contractor undertaking work on behalf of Aiming Higher and identifies the main principles of the DPA and GDPR that must be adhered to when processing personal information by, or on behalf of Aiming Higher. This will include all paper based and IT based information.

Purpose

The purpose of this policy is to ensure that the Aiming Higher's workforce, volunteers and students are aware of the principles of the DPA and GDPR and how this will influence their roles and responsibilities. The policy also defines the criteria and controls that must be applied throughout the Company to ensure compliance with legislation, regulations and operational good practice.

Responsibilities

Our management recognises their overall responsibility for ensuring that Aiming Higher complies with its legal obligations.

A Data Protection Officer will be appointed and will have the following responsibilities:

- briefing the board on data protection responsibilities,
- reviewing data protection and related policies,

Page 3 of 11

231-233 Church Street, Blackpool FY1 3PB Telephone: 01253 206448

Email: info@aiminghighercharity.org.uk Reg Charity: 1144664



- advising other employees on data protection issues,
- ensuring that data protection induction and training takes place,
- handling subject access requests,
- approving unusual or controversial disclosures of personal data,
- ensuring contracts with data processors have appropriate data protection clauses,
- electronic security,
- approving data protection-related statements on publicity materials and letters.

Each individual representative of Aiming Higher who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good data protection practice is established and followed.

The workforce is required to read, demonstrate their understanding and comply with all policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be subject to Aiming Higher's disciplinary procedures and could result in verbal or written warnings and dismissal.

DPA and GDPR Overview

The principles of data protection require that the personal data held by the company must be:

- fairly and lawfully processed (not processed unless specific conditions are met).
- processed for the purpose(s) obtained and not further processed in any manner incompatible with that purpose(s).
- adequate (not excessive) and relevant.
- accurate and kept up to date.
- not kept longer than is necessary.
- processed in accordance with the rights of data subjects.
- held in a secure manner.

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) have some key differences which may impact the UK's relationship with the EU, post-Brexit. The GDPR became enforceable on 25 May 2018. As a European regulation, it is directly effective in EU Member States, meaning that all UK organisations must comply with it until notified of any changes post Brexit.



The GDPR does however give Member States limited scope to shape how certain aspects of the Regulation apply in their country. The DPA 2018 enacts the GDPR into UK law, and in doing so has included various 'derogations' as permitted by the GDPR, resulting in some key differences.

Subtle Differences Between the DPA and GDPR

Child consent

- The GDPR states that a child can consent to data processing at age 16, whilst the DPA sets this at 13.

Extended definition of 'identifier'

- The GDPR extends the meaning of 'identifier' to include IP addresses, internet cookies and DNA in the definition of personal data

Criminal data

- The GDPR requires those processing criminal data to have official authority, the DPA does not.

Automated decision making/processing

- The GDPR states that data subjects have a right not to be subject to automated decision making or profiling, whereas the DPA allows for this whenever there are legitimate grounds for doing so and safeguards are in place to protect individual rights and freedoms.

Data subject rights

- The GDPR ensures that all data subjects have rights in relation to the processing of their personal data.
- The DPA allows these rights to be ignored if compliance with these rights would seriously impact an organisation's ability to carry out their functions when processing data for scientific, historical, statistical and archiving purposes.

Privacy vs Freedom of Expression

- The GDPR gives Member States scope to balance the right to privacy with the right to freedom of expression and information.
- The DPA provides an exemption from certain requirements of personal data protection in respect of personal data processed for publication in the public interest.

Differences between DPA and GDPR

The DPA is wider in scope than the GDPR, covering:



- criminal sanctions and fines for GDPR infringements (for example the introduction of an unlimited fine for the new offence of intentionally or recklessly re-identifying individuals from anonymised data)
- processing relating to areas outside the scope of EU law (and the GDPR) such as national security and immigration
- transposition of the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into UK law
- the role and powers of the UK's independent authority (the ICO) in upholding information rights and freedoms

As the GDPR is governed by the Court of Justice of the European Union (CJEU), now that the UK has left the EU, the DPA will be governed solely by the UK justice system.

Compliance

To comply with the principles of the DPA, Aiming Higher will:

- collect and use data fairly and lawfully.
- meet the legal obligations to specify the purpose for which information is used.
- collect and process appropriate information only to the extent that is needed to fulfil operational needs, or to comply with any legal requirements.
- only hold the data for an appropriate length of time.
- ensure that data subjects are able to fully exercise their rights under the DPA and this will include:
 - the right to be informed that the processing is being undertaken.
 - the right of access to their personal information.
 - the right to prevent processing in certain circumstances.
 - the right to correct, rectify, block or erase incorrect information.
- take appropriate security measures to safeguard personal information including:
- access to computer records containing personal information will be restricted to those persons who need access, in order to carry out their duties.
- personal information contained on paper files will be stored in locked cabinets and access restricted to those with a legitimate business need to access the data.



- instructing staff that material is not to be taken off site without express prior approval, or stored on personal machines normally kept outside the workplace

Data Recording and Storage

Aiming Higher operates electronic systems holding information about clients. Information on employees, volunteers and students may be held in paper form and electronic databases.

Aiming Higher will regularly review its procedures for ensuring that its records remain accurate and consistent and in particular:

- case management and database systems are reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- data on any individual will be held in as few places as necessary, and all employees.
- volunteers and students will be discouraged from establishing unnecessary additional data sets.
- effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- employees, volunteers and students who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.
- data will be corrected if shown to be inaccurate.

Aiming Higher stores archived paper records of clients, employees, volunteers and students securely in locked cabinets and secure archiving facilities.

Destroying Data

Once electronic records are no longer required, they are deleted from our databases and purged to remove all trace. Please see our data register for retention times for different data types.

Hard copy documents are shredded, on site.

Access to Data

All clients have the right to request access to all information stored about them. Any subject access requests will be handled by the Data Protection Officer within the required time limit.



Subject access requests must be in writing. All employees and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

All those making a subject access request will be asked to identify any other individuals who may also hold information about them, so that this data can be retrieved.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.

The required information will be provided in hardcopy format unless the applicant makes a specific request to be given supervised access in person.

Aiming Higher will provide clients' own personal details to those who request it unless the information may cause harm to another person.

Employees, volunteers and students have the right to access their personnel file to ensure that information is being used fairly. If information held is inaccurate, the individual must notify the Data Protection Officer so that this breach can be recorded on file and the personal data should be amended.

Transparency

Aiming Higher is committed to ensuring that, in principle, Data Subjects are aware that their data is being processed and:

- for what purpose it is being processed,
- the types of disclosure that are likely, eg safeguarding
- how to exercise their rights in relation to the data,
- data subjects will generally be informed in the following ways:
 - Employees: in Employment Terms and Conditions,
 - Trustees: in the Trustee Welcome/Support Pack,
 - Volunteers: in the Volunteer Welcome/Support Pack,
 - Service users: when they request services (in writing, online or by phone).

Standard statements will be provided to employees for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.



Consent

Consent will normally not be sought for most of the processing of information concerning trustees and the workforce. However, details will only be disclosed for purposes unrelated to their duties with Aiming Higher (eg financial references) with their consent.

Information about volunteers will be made public according to their role, and consent will be sought for:

- the means of contact they prefer to be made public, and
- any publication of information which is not essential for their role,
- the use of photographs and videos on social media and other publicity material.

Information about clients will only be made public with their consent and this includes photographs.

‘Sensitive’ data about clients (including health information) will be held only with the knowledge and consent of the individual.

Consent should be given in writing, although for some cases it is not always possible to do so eg in medical emergencies. Wherever possible, at least verbal consent will be sought to the storing, processing and sharing of data. In all cases it will be documented on the database that consent has been given.

All Data Subjects will be given the opportunity to opt out of their data being used in particular ways, such as the right to opt out of direct marketing.

Aiming Higher acknowledges that once given, consent can be withdrawn, but not retrospectively. There may be occasions where Aiming Higher has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn by the data subject. There may be legal or contractual obligations for retaining this data.

Direct Marketing

Aiming Higher will treat the following unsolicited direct communication with individuals as marketing:

- promoting any Aiming Higher services
- promoting Aiming Higher events
- marketing the products of Aiming Higher
- marketing on behalf of any other external company or voluntary organisation.

Whenever data is first collected, which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given an opt out option. If it is not possible to give a range of options, any



opt-out which is exercised will apply to all Aiming Higher marketing. Aiming Higher does not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings and so will never do so.

Aiming Higher will only carry out telephone marketing where consent has been given in advance, or the number being called has been checked against the Telephone Preference Service.

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

Employees, Volunteer and Student Training and acceptance of responsibilities

All employees, volunteers and students who have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, including the Data Protection Policy, Confidentiality Policy and the operational procedures for handling personal data. The workforce must comply with all these policies and procedures.

Induction Training

Aiming Higher will provide opportunities for employees, volunteers and students to explore Data Protection issues through training, team meetings, and supervisions.

When an individual requests information from Aiming Higher, signs up to any of our services, Aiming Higher obtains information about the individuals who will benefit from those services.

This statement explains how we look after that information and what we do with it.

Aiming Higher has a legal duty under the DPA and GDPR to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally, the only information we hold comes directly from you or from an organisation to which you have given your consent to share your information with us. Whenever we collect information from you, we will make it clear which information is required in order to provide you with the information, services or goods you need. You do not have to provide us with any additional information unless you choose to do so.

We store your information securely on our computer system and restrict access only to those persons who have a need to know. Our workforce and representatives are fully trained in handling your information securely.

If you have signed up to a service, we will pass your details to the professional worker providing that service. That worker may gather and record additional information about your circumstances, health and wellbeing on a regular basis so that we can ensure you always receive the best possible service from us.

We may wish to contact you in the future to tell you about other services we provide, to keep you informed of what we are doing and ways in which you might like to engage with Aiming Higher. You have the right to ask us not to contact you in this way. We will always aim to provide a clear method for you to opt out. You can also contact us directly at any time to tell us not to send you any future marketing materials.



Very occasionally, we may carry out a joint mailing, with carefully selected partner organisations, in order to tell you about products and services we think you might be interested in. Again, you have the right to opt out of this.

You have the right to request a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you). To obtain a copy of this information, either contact us by telephone on **01253 376200** to request an application form to be sent to you or write to:

The Data Protection Officer
Aiming Higher
231-233 Church Street
Blackpool FY 3PB

There is a charge of £10 for a copy of your data (as permitted by law) and this payment should accompany your letter of request. Cheques should be made payable to Aiming Higher. We aim to reply as promptly as we can and, in any case, within the legal maximum of 40 days.

Policy Review

The policy will be reviewed annually and approved by the Board of Trustees. It will also be reviewed in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.

