Data Protection Policy

Key details:

Prepared by: Mark Ellis
Approved on: 14th September 2017
Next review date: 14th September 2018

Introduction

Aimhigher London South needs to gather and process information about individuals. We collect a wide range of personal data from the participants of the activities we organise in order to be able to evaluate the impact of these activities. Sharing this data with the members of our organisation in order to demonstrate that we are correctly targeting our activities and that our activities have impact is a core business process. In the case of government funded projects it is a requirement of the contract with the government body that distributes the funds. Some of the personal data we collect is classified as 'sensitive' eg ethnicity and disability, and therefore it needs to be treated with greater care than other personal data. We also collect personal data from the parents/guardians of the participants of our activities, other people the organisation has a relationship with or may need to contact, and its employees.

Why this policy exists

This data protection policy ensures Aimhigher London South:

- Complies with data protection law and follow good practice
- Protects the rights of staff and participants of events
- Is open about how it stores and processes individual's data
- Protects itself from the risk of a data breach

Data Protection Law

The Data Protection Law 1998 describes how organisations – including Aimhigher London South - must collect handle and store personal information. The rules apply regardless of 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.

The data Protection Act is underpinned by eight important principles. These say that personal data must :

- Be processed fairly and lawfully
- Be obtained only for specific lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary.
- Processed in accordance with the rights of data subjects

- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA) unless the country or territory also ensures an adequate level of protection.

People, risks, and responsibilities

Policy scope

This policy applies to:

- The office of Aimhigher London South
- All staff and volunteers of Aimhigher London South
- All student ambassadors working for Aimhigher London South
- All contactors suppliers and other people working on behalf of Aimhigher London South

It applies to all data that the company holds in relation to identifiable individuals even if the information technically falls outside of the Data Protection Act 1998. It can include

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

Data Protection Risks

This policy helps to protect Aimhigher London South from some very real data security risks, including:

- Breaches of confidentiality. For instance data given out inappropriately
- Failing to offer free 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 Aimhigher London South has some responsibility for ensuring data is collected, stored and handled appropriately. Everyone that handles data must ensure that it is handled and processed in line with this policy and data protection principles. However the directors are ultimately responsible for ensure that Aimhigher London South meets its legal obligations.

General Staff Guidelines

The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. When access to confidential information is required employees can request it from their line managers.

Aimhigher London South will provide training to all employees to help them understand duties responsibilities when handling data. As part of their induction, new employees should be asked to read this document and also Kingston University's Data Protection Policy Section 1.13

Employees should keep all data secure by taking sensible precautions and following the guidelines below. In particular strong passwords must be used and they should never be shared. Personal data must not be disclosed to unauthorised people within the company or externally.

Employees should request help from their line manager if they are unsure about any aspect of data protection

Data collection

The basis on which data is being collected and processed must be made clear to those asked for it.

Where the basis for collection of data is consent, a privacy notice which includes an explanation of why the data is being collected and how it will be used should be issued before consent is requested. The communication used should be age appropriate so it can be easily understood by the participant.

In addition, the length of time the data will be held, how consent can be withdrawn, and how a complaint about the use of the data can be made should be included in the privacy notice.

Parental consent must be sought in addition to participants' consent if participants are under 16 (until the law concerning the need for parental consent has been clarified) and sensitive information is being requested via the participants' school. Consent of parents to share their children's sensitive data may be collected verbally by schools provided that there is a clear record of the basis on which the data was collected, how and when it was collected, and by whom.

Consent must be actively and freely given and recognition of imbalances of power between data collectors and participants should be taken into account. It must be sought at the point of delivery wherever possible.

When there is a requirement for the collection of new forms of data or the collection of the same data in a new way (as a result of a new project, or Government initiative which Aimhigher London South is tasked with carrying out for example), a Data Protection Impact Assessment should be considered if the data processing is likely to result in a high risk to individuals.

Data Storage.

A record of the data that Aimhigher London South holds should include where it is, where it came from and who it has been shared with. This record should be regularly reviewed (yearly?) and updated. If data is found to be out of date or no longer required it should be deleted and disposed of.

These rules describe how and where data should be safely stored. These guidelines apply to data that is usually stored electronically but has been printed out for some reason.

- When data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly and never shared between employees
- If data is stored on removable media like a CD or DVD these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones
- When data is stored on paper it should be keep in a secure place where unauthorised people cannot see it
- Data printouts should be shredded and disposed of securely when no longer required
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer
- Data processed for academic research should be deleted after 10 years, all other data should be deleted 6 years after it is collected unless there is a clear business reason for keeping it.
- When hardware which has contained data is no longer needed, care should be taken to professionally erase all trace of that data before the equipment is disposed of
- As all of our data is stored on the premises or the servers of Kingston University, in the case of a breach of data protection a DPA Notification Online Form should be filled out on Kingston University's website as soon as a member of staff becomes aware of this
- If a breach of data protection takes place in the transmission of data to another organisation, the ICO should be informed

Data use

Personal data is of no value to Aimhigher London South 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 should ensure the screens of their computers are always locked when left unattended
- Sensitive personal data should not be shared informally. In particular it should never be sent by email, as this form of communication is not secure
- Data must be encrypted before being transferred electronically. The use of a secure sharing site such as Kingston University's Box should be used to pass data from one organisation to another.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data
- Before data is shared with another organisation, a copy of the organisation's own data protection policy should be requested.

- Consent to share with this organisation must be sought from the person who gives us their data at the point they give it to us.

Data accuracy

The law requires Aimhigher London South:

- 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 Aimhigher London South should 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 should not create any unnecessary additional data sets
- Staff should take every opportunity to ensure data is updated
- Data should be updated as inaccuracies are discovered. For instance, if a teacher can no longer be reached on their stored phone number it should be removed from data records

Subject access requests

All individuals who are the subject of personal data held by Aimhigher London South are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how it is kept up to date
- Be informed how the company is meeting its data protection obligations
- Be informed of their right to complain to the IOC if they think that the way their data is being used breaches the Data Protection Act 1998

If an individual contacts the company requesting this information it is called a subject access request
Subject access requests from an individual should be made by email, addressed to one of the directors of the company, Catherine Fenwick at c.fenwick@kingston.ac.uk , or Suzanne Marchment at s.marchment@kingston.ac.uk

- The company will aim to provide the relevant data within 21 days.
- The person dealing with the request will always verify the identity of anyone making a subject access request before handing over any information
- Where the request is refused, the individual must be informed of the reason why and their recourse to the IOC if they are unhappy with the response

Disclosing data for other reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances Aimhigher London South will

disclose requested data. However the company will ensure the request is legitimate, seeking assistance from the the company's legal advisers where necessary.