HARROW INDEPENDENT COLLEGE

School of Mathematics, Science & Economics

Data Protection Policy of Harrow Independent College

Introduction

Harrow Independent College (HIC) uses certain types of information relating to Data Subjects who come into contact with the college. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material to ensure compliance with the Data Protection Act 1998 as well as the General Data Protection Regulation 2018 (GDPR).

1. Data Controller

HIC is the Data Controller under the Act, which means that it determines what purpose personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purpose that this data will be used for. The college's registration number is ZA163536.

2. Disclosure

HIC may share data with other agencies such as the local authority (LA), educational support providers and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law permits HIC to disclose data (including sensitive personal data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of a Data Subject or other person
- The Data Subject has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion

HIC regards the lawful and correct treatment of personal information as important to successful working, and to maintaining the confidence of those with whom we deal.

HIC intends to ensure that personal information is treated lawfully and correctly.

To this end, the college will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998 or GDPR 2018.

Specifically, the Principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

b) Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

c) Shall be adequate, relevant and not excessive in relation to those purpose(s)

d) Shall be accurate and, where necessary, kept up to date,

e) Shall not be kept for longer than is necessary,

f) Shall be processed in accordance with the rights of data subjects under the Act,

g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of the Data Subject in relation to the processing of personal information.

HIC will, through appropriate management and strict application of criteria and controls**:**

- Observe fully, conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as incorrect
- Take appropriate technical and organisational security measures to safeguard personal information

- Ensure that personal information is not transferred abroad without suitable safeguards

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information

- Set out clear procedures for responding to requests for information

3. Data collection

Informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data

- And then gives their consent.

HIC will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing an electronic or paper form.

When collecting data, HIC will ensure that the Data Subject:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

e) Has received sufficient information on why their data is needed and how it will be used

4. Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is the responsibility of HIC to ensure all personal and company data is non-recoverable once deemed to be redundant. This includes both paper-based copies as well as copies held on any computer system previously used within the organisation and/or which has

been passed on to a third party.

5. Data access and accuracy

All Data Subjects have the right to access the information HIC holds about them. HIC will also take reasonable steps to ensure that their information is kept up to date by asking data subjects whether there have been any changes.

In addition, HIC will ensure that:

- It has a Data Protection Officer (DPO) with specific responsibility for ensuring compliance with Data Protection. Currently the DPO is Mr Kandiah Kandeepan who holds the position of the Principal of the college

- Everyone processing personal information understands that they are contractually responsible for following good data protection practices

- Everyone processing personal information is appropriately trained to do so

- Anybody wanting to make an enquiry about handling personal information knows what to do and those persons deals promptly and courteously with any enquiries about handling personal information

- All staff describes clearly how to handle personal information

- All staff will regularly review and audit the ways it holds, manages and uses personal information

- All staff regularly assesses and evaluates methods and performance in relation to handling personal information

- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 or GDPR 2018.

Policy Reviewed – 15th May 2019

Next Review – 15th May 2020

Glossary of Terms

Data Controller – The Data Controller is 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.

Data Subject – The data subject is the individual whom particular personal data is about.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

General Data Protection Regulation 2018 (GDPR) – The new legal framework introduced by the European Union. These regulations will replace the Data Protection Act 1998 on the 25th of May 2018.

Data Protection Officer (DPO) – The person(s) responsible for ensuring that HIC follows its data protection policy and complies with the Data Protection Act 1998 or GDPR 2018.

Explicit consent – is a freely given, specific and informed agreement by a Data Subject in the processing of personal information about her/him. Explicit consent is needed for processing sensitive personal data.

Notification – Notifying the Information Commissioner about the data processing activities of HIC, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self-assessment guide will help you to decide if you are exempt from notification:
https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees.

Sensitive personal data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings