LIPA SIXTH FORM COLLEGE

Data Protection Policy

Introduction

This describes how we manage data protection.

This applies to staff and students in all cases where we are the data controller or a data processor of personal data. It applies regardless of who created the data, where it is held or the ownership of the equipment used.

We obtain, use, store and process personal data for:

- potential staff, students and pupils (applicants);
- current staff, students and pupils;
- former staff, students and pupils;
- current and former workers and contractors;
- governors;
- visitors;
- website users; and
- contacts.

These are collectively referred to as data subjects. When processing personal data, we are obliged to fulfil individuals' reasonable expectations of privacy, complying with GDPR and other relevant data protection legislation (data protection law).

Responsibilities under the Policy

We must adhere to the six Data Protection Principles ("the Principles") as set out in the legislation. These six principles are:

These principles require personal data to be:

1. Processed lawfully, fairly and in a transparent manner;

2. Collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

4. Accurate and where necessary kept up to date;

5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed;

6. Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Data Security

All users of personal data must ensure that personal data are always held securely and are not disclosed to any unauthorised third party either accidentally, negligently or intentionally.

-

Privacy Notices

When we collect personal data from individuals, we must adhere to the principle for 'fairness and transparency'.

This means that we must provide data subjects with a 'privacy notice' to let them know how and for what purpose their personal data are processed.

Any data processing must be consistent or compatible with that purpose.

Privacy notices have been published in relation to:

- Visitors to our websites;
- Prospective students and pupils;
- Job applicants;
- Staff;
- Students;
- Alumni.

Conditions of Processing/Lawfulness

In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

- The data subject has given consent;
- The processing is required due to a contract;
- It is necessary due to a legal obligation;
- It is necessary to protect someone's vital interests (i.e. life or death situation);
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- It is necessary for the legitimate interests of the controller or a third party.

Data Retention

Personal data must not be kept longer than necessary.

After use, it must be securely destroyed or deleted.

Details of how long specific records are retained for is set out in our Records Retention Schedule.

Data Protection by Design and Default

Under the GDPR and the DPA, we have an obligation to consider the impact on data privacy during processing activities. This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy.

Data Protection Impact Assessment

When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the first stage and a Data Protection Impact Assessment (DPIA) conducted.

The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection control requirements are not an after-thought.

Responsibilities of Managers and Data Users

All managers have a responsibility to ensure compliance with the GDPR, the DPA and this policy and to develop and encourage good information handling practices within their areas of responsibility.

All users of personal data have a responsibility to ensure that they process the data in accordance with the six principles and the other conditions set down in the legislation.

Data Subject Rights

The GDPR and the Act contain eight data subject rights. These are the rights to:

- Information (privacy notices);
- Subject access;
- Rectification;
- Objection;
- Erasure:
- Portability;
- Restriction of processing; and
- Restriction of automated decision-making and profiling.

Subject Access Requests and the Right to Data Portability

Individuals have the right to request to see or receive copies of any information we hold about them, and in certain circumstances, to have that data provided in a structured, commonly used and machine readable format, so it can be forwarded to another data controller.

We must respond to these requests within four weeks. It is a personal criminal offence to delete relevant personal data after a subject access request has been received.

Individuals receiving a subject access request must contact our Data Protection Officer, Greg Parker g.parker@lipaprimary.org) straight away.

Right to erasure, to restrict processing, to rectification and to object

In certain circumstances, data subjects have the right to have their data erased.

This only applies:

- where the data is no longer required for the purpose for which it was originally collected; or
- where the data subject withdraws consent; or
- where the data is being processed unlawfully.

In some circumstances, data subjects may not wish to have their data erased, but rather have any further processing restricted.

If personal data is inaccurate, data subjects have the right to require us to rectify inaccuracies. In some circumstances, if personal data are incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

Data subjects have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

Individuals receiving any of these requests should not respond but instead should contact the Data Protection Officer immediately.

Rights in relation to automated decision making and profiling

In the case of automated decision-making and profiling that may have significant effects on data subjects, data subjects have the right to either have the decision reviewed by a human being or to not be subject to this type of decision making at all. These requests must be forwarded to the Data Protection Officer immediately.

Data Sharing

When personal data is transferred internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected.

If personal data is shared internally for a new and different purpose, a new privacy notice will need to be provided to the data subject(s).

When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between us and the third party must be signed, unless disclosure is required by law, such as HMRC, or the third party requires the data for law enforcement purposes.

Transfers of Personal Data outside the EEA

Staff are not permitted to store or transfer your data outside of the EU.

Direct Marketing

Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals.

For us, this will include notifications about events, fundraising, selling goods or services.

Marketing covers all forms of communications, such as contact by post, fax, telephone and electronic messages, whereby the use of electronic means such as e-mails and text messaging is governed by the Privacy and Electronic Communications Regulations 2003.

We must ensure that we always comply with relevant legislation every time we undertake direct marketing and must stop all direct marketing activities if an individual requests it to stop.

Data Protection Training

It is mandatory for all staff members to complete the Data Protection Training module.

Data Breaches

We are responsible for ensuring appropriate and proportionate security for the personal data that we hold.

This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data.

We make every effort to avoid data breaches. However, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment;

- Ineffective access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. e-mail sent to the incorrect recipient);
- Human error;
- Hacking attack.

Any data protection incident must immediately be brought to the attention of our Data Protection Officer.

The Data Protection Officer will immediately investigate and decide if the incident constitutes a data protection breach.

If a reportable data protection breach occurs, we are required to notify the Information Commissioner's Office as soon as possible and not later than 72 hours after becoming aware of it.