Data Protection Policy

REVISION NUMBER	REVISION DATE	REVISION(S) MADE	REVISION APPROVAL DATE
1	September 2018	Revised by DPO following GDPR	

Author: Mr N Malik – Data Protection Officer

Last Reviewed: September 2018

Next review Date: September 2019

Introduction

1. Definition of data protection terms
2. The GDPR key principles
3. Lawful basis for processing
4. Data protection by design and by default
5. Data protection Impact assessment
6. The rights of the individuals
7. Data breaches
8. Consent
9. Subject access requests
10. CCTV and photography
11. Data sharing
12. Data retention

Introduction

Laurus Trust is committed to data protection by design and regards the lawful and correct processing of personal and special category data as an integral part of its purpose.

This policy sets out the accountability and responsibilities of the School, its staff and its students to comply fully with the provisions of the General Data Protection Regulation and the Data Protection Act 2018.

Laurus Trust holds and processes personal data about individuals such as employees, students and others, defined as 'data subjects'. Such data must only be processed in accordance with the GDPR and the DPA.

Laurus Trust has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with the GDPR and the DPA.

Laurus Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, the local authority, other schools and educational bodies, and potentially children's services.

The Digital Economy Act 2017 requires every data controller (i.e. organisation) in the UK to pay a fee to the Information Commissioner's Office (ICO). The schools registration number is Z5543382.

1. Definition of data protection terms

1. Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

2. Data subjects for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3. Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

4. Data controllers are the people who or organisations that determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our School for our school purposes.

5. Data processors include any person or organisation that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the schools behalf.

6. Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

7. Special category data includes information about a person's race, ethnic origin, political opinions, religion, trade union membership, genetics, Biometrics (where used for ID), health, sexual life, or Sexual orientation.

2. The GDPR sets out seven key principles for processing data

1. Lawfulness, fairness and transparency

2. Purpose limitation

3. Data minimisation

4. Accuracy

5. Storage limitation

6. Integrity and confidentiality (security)

7. Accountability

3. The lawful bases for processing

are set out in Article 6 of the GDPR. At least one of these must apply whenever the school processes personal data.

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

4. Vital interests: the processing is necessary to protect someone's life.

5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

4. Data protection by design and default.

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

5. 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 earliest stage and a Data Protection Impact Assessment (DPIA) must be 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.

6. Rights of the data subject

The GDPR was designed to strengthen the privacy rights of individuals. It offers more control to the data subject over what happens to their personal data, this has been expressed in GDPR under the following eight rights:

The Right to be informed

The right to be informed covers some of the key transparency requirements of the GDPR, namely the first principle which promotes fair and transparent processing of personal data. Essentially, it' is about being as clear and concise as possible with the data subject and inform them how and why their information is being used.

The Right of Access

The right of access, commonly referred to as subject access, essentially gives individuals the right to obtain a copy of all their personal information. It helps individuals to understand how and why you are using their data, and also to check you are doing so lawfully.

The Right to Rectification

As expected, the right to rectification allows an individual to have any inaccurate information rectified. An individual may also be able to have incomplete personal data completed, although this depends on the purposes for the processing. This is closely linked to the 'Accuracy' principle of GDPR, however although steps may have been taken to ensure that personal data was accurate when you obtained it, this right requires reconsideration of the accuracy upon request.

The Right to Erasure

The right to erasure, commonly referred to as, 'the right to be forgotten', gives individuals the right to have their personal data erased. However this is not an absolute right and only applies in certain circumstances. A few examples of instances where it could apply would be:

i. If the personal data is no longer necessary for the purpose for which it was originally collected

ii. If 'consent' is the lawful basis for holding the data, and the individual withdraws their consent

iii. You have processed the personal data unlawfully

The Right to Restrict Processing

This right allows an individual to restrict the processing of their data. This means they can limit the way an organisation uses their data, and can be thought of as an alternative to requesting the erasure. Similarly, this can only be applied in certain circumstances such as:

i. When the individual contests the accuracy of their personal data and you are in the process of verifying this accuracy.

ii. The data has been processed unlawfully, and instead of erasure, the individual request restriction instead.

iii. You no longer need the personal data, but the individual requests you keep it in order to establish, exercise or defend a legal claim.

The Right to Data Portability

The right to data portability essentially gives individuals the right to have any data they have 'provided' to a controller to be moved between data controllers. This right only applies when the lawful basis for processing the information is either consent or for the performance of a contract. It also only applies to processing carried out digitally (i.e. this excludes paper files). The definition of 'provided to a controller' doesn't just mean direct information given to the controller, it can also mean personal data resulting from observation of an individual's activities.

This may include:

i. History of website usage or search activities;

ii. Traffic and location data; or

iii. 'Raw' data processed by connected objects such as smart meters and wearable devices.

The Right to Object

This right gives individuals the right to object to the processing of their personal data, effectively asking the organisation to stop processing it. Again this can only be used in certain circumstances and depends on the purposes and lawful basis used for processing.

An example of when this right can be applied is when:

Personal data is being used for direct marketing purposes and the individual wishes to object to this.

However, as stated this right isn't absolute and will need to be carefully weighed up between the organisations' justification for processing the information, and the rights and freedoms of the individual.

The Rights to Automated Decision Making

GDPR has provisions on decisions which are made solely by automated means without any human involvement, and profiling (automated processing of data to evaluate certain things about an individual).

Examples of this would be:

i. An online decision to award a loan.

ii. Or a recruitment aptitude test which uses pre-programmed algorithms and criteria.

GDPR restricts you from making solely automated decisions, included those based on profiling, that have a legal or similarly significant effect on an individual. The type of effect isn't specifically defined in GDPR however the decision must have a serious negative impact on an individual to be under the remit of this provision.

7. Data Protection Breaches

Laurus Trust is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The School makes every effort to avoid data protection incidents, 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. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any data protection incident must be brought to the attention of the Schools Information Governance Team who will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, the school is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after becoming aware of it. Any member of the school who encounters something they believe may be a data protection incident must report it immediately.

8. Consent

The GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement between the school, parents and pupils.

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Laurus Trust will keep clear records to demonstrate where consent has been given.

The GDPR gives a specific right to withdraw consent. You can withdraw consent where given at any time by contacting us on dataprotection@laurustrust.co.uk

9. Data Subject Access Requests

Data subjects have the right to receive a copy of their personal data which is held by the School. In addition, an individual is entitled to receive further information about the Schools processing of their personal data as follows:

1. the purposes

2. the categories of personal data being processed

3. recipients/categories of recipient

4. retention periods

5. information about their rights

6. the right to complain to the ICO,

7. details of the relevant safeguards where personal data is transferred outside the EEA

8. any third-party source of the personal data

10. CCTV and photography

Laurus Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

All CCTV footage will be kept for 14 days for security purposes.

If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written consent will be sought for the particular usage from the parent or guardian of the pupil.

Images captured by individuals for their domestic purposes, and videos made by parents for family use, are exempt from the GDPR.

11. 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 students.

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

12. Data retention

1. We will not keep your data for longer than is necessary.

2. Your data will be retained and processed as prescribed in our retention policy and privacy notice.

3. Paper records will be securely shredded/destroyed once it is no longer needed.