



DATA PROTECTION POLICY

Author - M Vevers

Last reviewed - July 2015

Next review date - July 2017

Reviewed by -

The Laurus Trust Data Protection Policy

Definitions

As in the Data Protection Act 1998 (the Act), for the purposes of this policy Laurus Trust is the 'data controller'; 'data means information which is being processed by means of equipment operating automatically in response to instructions given for that purpose and is recorded with the intention that it should be processed by means of such equipment'; 'personal data' means data which relate to a living, identifiable individual; 'data subject' means the individual who is the subject of the personal data; and 'processing' means anything done to the personal data including simply holding it.

Introduction

The Laurus Trust collects and uses certain types of personal data about staff, students, parents and other individuals who come into contact with the academy schools within the Trust in order to provide education and associated functions. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Education Authorities (LAs), government agencies and other bodies.

This policy is intended to ensure that personal data are processed in accordance with the Act and other related legislation. It applies to personal data regardless of the way they are used, recorded and stored and whether they are held in paper files or electronically.

Data Protection Principles

The Act contains eight data protection principles of good information handling which must be followed at all times. They require data controllers to ensure that:

- personal data are processed fairly and lawfully;
- personal data are obtained only for one or more specified and lawful purposes;
- personal data are adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;
- personal data are accurate and where necessary kept up to date;
- personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose;
- personal data are processed in accordance with the rights given to data subjects under the Act;
- appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and
- personal data are not transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Laurus Trust is committed to complying with these principles at all times.

This means that the Laurus Trust will:

- tell you what purposes we will use personal data for when we collect them;
- tell you if personal data will be shared, as well as telling you why, with whom and under what circumstances. Any data shared will be kept secure at all times and permission will be sought, where necessary, prior to any personal information being included on any of the Trust's websites;
- inform staff, students and visitors why we are collecting personal information by CCTV images and will regularly review the retention periods of this specific data. CCTV cameras will only be sited where they are needed for a stated purpose and will not intrude on anyone's privacy;
- check the quality and accuracy of the personal data we hold;
- apply our records management policies and procedures to ensure that personal data are not held for longer than is necessary;
- ensure that when personal data are authorised for disposal it is done appropriately;
- ensure appropriate security measures are in place to safeguard personal data, whether they are held in paper files or on our computer system. All confidential information will be kept secure when storing it, using it and sharing it with others;
- share personal data with others when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests from data subjects who want access to the personal data we hold about them. These requests are known as 'subject access requests' under the Act; and
- train our staff and Governors so that they are aware of our policies and procedures.

This policy will be updated as necessary to reflect best practice or amendments made to the Act.

Complaints

Complaints under this policy should be made to the Chairperson of the Governing Body who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. Complaints which are not dealt with under the Trust's complaints procedure may be eligible for investigation by the Information Commissioner's Office (ICO). The ICO can only consider complaints about possible contraventions of the Act and any complaint must be submitted in writing. Further information about submitting a complaint to the ICO is available at www.ico.gov.uk. It is likely that complaints about procedural issues, due process and timeliness will be dealt with by the trustees.

Contacts

If you have any concerns or questions in relation to this policy please contact the IG Lead (trustee) who will also act as the contact point for any subject access requests made under the Act.

Further general advice and information about the Act and related legislation is available from www.ico.gov.uk.

This policy should be read in conjunction with the Privacy Notice.

Appendix 1

The Laurus Trust

Procedures for responding to subject access requests in accordance with the Data Protection Act 1998

Anybody who makes a request to see or be provided with a permanent copy of their file, their child's file or any other data about them processed by the Trust is making a subject access request (SAR) under the Data Protection Act 1998 (the Act). All information relating to the data subject including that held in day books, diaries, electronic systems, CCTV images and email should be considered for disclosure.

Normally a parent or guardian can only make a SAR for their child's personal data if the child is under 12 years of age and it is clear the parent is acting in the child's interests. The general view is that children aged 12 or above are capable of understanding the process; therefore in these cases the child's written consent is needed before providing his or her personal data to a parent. There will be instances where older children are not capable of giving informed consent; these SARs should be assessed on a case by case basis.

There is a statutory exception to the above which gives parents the independent right to access their child's official education record regardless of whether or not their child consents. Parents are given this right under The Education (Pupil Information) (England) Regulations 2000 and 2005 (the Regulations). CHHS will observe these statutory rights; however the Regulations **do not** give the parent the right to access personal data which do not form part of their child's official education record.

If there is a current court order which relates to information regarding any child, regardless of other circumstances, that order must be observed.

Dealing with a subject access request

A SAR or request for an education record must be made in writing and a response provided within the statutory time limit. Data controllers have 40 calendar days to respond to SARs; however where the request concerns education records (made by parents or pupils under the Regulations or as part of a SAR under the Act) a response must be provided within 15 school days.

The 'first day' of the response period does not start until the data controller is provided with any required fee up to the statutory maximum, any information it may reasonably require in order to locate the information requested and information to satisfy itself as to the identity of the requester. This can be done in a variety of ways; however asking to see photographic ID e.g. passport or driving licence is most appropriate. If a parent or other individual is making a request for a child's personal data, the Trust should also be satisfied that there is a legitimate relationship between the requester and the child and that they are acting in the child's interests. **Any further information of the above nature will be obtained from the requester without delay.**

The IG Lead (trustee) will have responsibility for ensuring the child's welfare is appropriately considered when deciding whether or not to comply with a request. Normally the requester will have to prove both their relationship with the child and that disclosure is in the child's best interests, to the satisfaction of the IG Lead.

The Trust may charge a fee up to the statutory maximum in order to comply with SARs. The maximum fee for SARs is £10; however where the request (either under the Act or the Regulations) involves education records, fees are calculated on a sliding scale dependent on the number of pages involved. These fees only apply if a permanent copy of the education record is provided.

In certain circumstances, personal data are exempt from SARs and the Trust will make use of applicable exemptions under the Act as appropriate. All files must be reviewed before any disclosure takes place. Under no circumstance will access be granted immediately or before this review process has taken place.

In some cases, the Trust will hold information which has been provided to it by a third party e.g. the local authority, the police, a health care professional or another school. If this information is the personal data of a third party individual, it is normal practice to obtain the consent of the third party before disclosing their personal data. This will be done as soon as possible to ensure you respond to the SAR within the statutory time limit. Even if the third party does not provide their consent, the personal data may still be disclosed legitimately in certain circumstances. In these cases, the Trust may seek additional advice.

In the response the requester should be given: a description of the information the Trust holds; a copy of the personal data; an explanation of the purposes for which they are processed; and an explanation of whether they have been shared with any other party. It is good practice to explain whether personal data have been withheld and if so, why. There may be circumstances where this is not appropriate and the IG Lead should consider the welfare of the child at all times.

If a document contains information that cannot be disclosed, a permanent copy will be made with the withheld data obscured. In certain circumstances the personal data being disclosed will be re-typed if this is more sensible. In any event a copy of the original full document (before redaction) and the amended document should be retained together, with an explanation of why the document was redacted. This is so that in the event of a complaint there is an audit trail detailing what was done and why. In addition, any codes, technical terms or abbreviations should be explained and a transcript of any personal data which are difficult to read or are illegible should be provided with the copy of the original document.

In its response, the Trust will also provide details of who to contact in the event of a complaint. This may be the Chair of Governors or the LEA. It is also helpful to provide the contact details of the ICO which can provide independent advice and information about the legislation.

Responses to SARs will be posted by Special Delivery or if the requester agrees, they can be left at the academy schools for collection with an officer available to help if required. If the response has been compiled for inspection only with the prior agreement of the requester, access to a photocopier will be provided in case they want a permanent copy of their personal data.

The Trust will monitor the number of requests received and document whether they are dealt with within statutory timescale.

Complaints

Complaints about the Trust's adherence to these procedures should be made to the Chairperson of the Governing Body who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. Complaints which are not dealt with under the

Trust's complaint procedure should be forwarded in writing to the ICO by the complainant. It is likely that complaints about procedural issues, due process and timeliness will be dealt with by the trustees. Complaints about alleged contraventions of the Act can be investigated by the ICO.

Contacts

If you have any concerns or questions in relation to this policy please contact the IG Lead who has responsibility for Information Governance.

September 2016