Data Protection

Document Detail	
Type of Document (Stat Policy/Policy/Procedure)	Policy
Category of Document (Trust HR-Fin-FM-Gen/Academy)	General
Index reference number	LAT-GEN-03-PO
Approved	April 2020
Approved by	Trust Board
Next Review date	April 2021
Version	V4

Date	Version	Revision Description
19/10/17	1	Adopted as a MAT
26/4/18	2	Complete revision in line with GDPR requirements
21/06/2019	3	Removal of references to CEO and Governors to bring into line with current Academy Structure
20/04/2020	4	Data Breach policy merged 3.1 – update to Data Protection Register date

Contents

Part 1 Introduction and Key Definitions

The definition of 'Trust' throughout this policy applies to Life Academies Trust and the Academies/Settings within it.

1.1 Introduction

LIFE Academies Trust needs to gather and use certain information about individuals.

These individuals can include pupils, parents/carers, employees, suppliers, business contacts and other people the Trust has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Trusts data protection standards — and to comply with the law.

This data protection policy ensures the Trust:

- complies with data protection law and follows good practice
- protects the rights of pupils, staff, parents/carers and other stakeholders
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

This Data Protection policy is based on the six principles of the Data Protection Act (DPA) that personal data shall be:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. accurate and kept up to date
5. kept in a form which permits identification of data subjects for no longer than is necessary
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or damage

1.2 Key Definitions

Data

The DPA describes how organisations, including the Trust, must collect, handle and store personal information ('data').

Data is any information that the school collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this. Sensitive data includes:

- racial or ethnic origin.
- political opinions.
- religious or philosophical beliefs.
- trade union membership.
- data concerning health or sex life and sexual orientation.
- genetic data; and
- biometric data.

Data can be 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.

Data Subject

A 'Data Subject' is someone whose details the Trust keeps on file. The data subject has the following rights under data protection legislation:

- to be informed
- to have access to data stored about them (or their children)
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for the school to keep their data
- to restrict processing (e.g. limit what their data is used for)
- to object to data being shared or collected

Although data protection legislation affords these rights to individuals, in some cases the obligations schools have to share data with the DfE etc. override these rights (this is documented later in the policy under 'Privacy Notices').

Data Controller

The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf.

The Trust is the 'Data Controller'.

Data Processor

A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff, Third Party Company or another organisation such as the police or Local Authority (LA).

Part 2 Organisational Arrangements

2.1 Overall Responsibility

Life Academies Trust will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

2.2 Roles & Responsibilities

Trust Board

The Trust Board will:

- Establish and maintain a positive data protection culture.
- Ensure that a Data Protection policy is approved by the Trust Board.
- Review and monitor the effectiveness of the policy.
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties.

- Allocate sufficient resources for data protection, e.g. in respect of training for staff, encryption technology for devices.
- Monitor and review data protection issues.
- Ensure adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Data Protection Officer.

Academy Principal

Academy Principal will:

- Prepare a Data Protection policy for approval by the Trust Board, revise as necessary and review on a regular basis, at least every two years
- Promote a positive data protection culture.
- Implement the Data Protection policy.
- Ensure that all staff co-operate with the policy.
- Coordinate training on data protection for all key stakeholders in the Trust.
- Carry out a data protection induction for all staff and keep records of that induction.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Monitor the work of the Data Protection Officer to ensure they are fulfilling their responsibilities.

Data Protection Officer

The Data Protection Officer will:

- Inform and advise the Trust of their obligations under data protection legislation.
- Monitor compliance with the legislation and report to the Academy Principal and Trust Board. There will be an audit and two updates by form of a written report annually.
- Cooperate with the supervisory authority (e.g. Information Commissioners Office) and act as the main contact point for any issues.
- Seek advice from other organisations or professionals, such as the Information Commissioners Office as and when necessary.
- Keep up to date with new developments in data protection issues for schools.
- Act upon information and advice on data protection and circulate to staff and trustees
- Have access to staff data protection induction records.
- Be made aware of any Subject Access Request and offer advice/represent the Trust as appropriate.
- Be made aware of any data breach and offer advice/represent the Trust as appropriate.

Trust Employees

Staff at the Trust will:

- Familiarise themselves and comply with the Data Protection Policy.
- Comply with the Trust data protection arrangements.
- Follow the data breach reporting process.
- Attend data protection training as organised by the Trust.

Part 3 Detailed Arrangements & Procedures

3.1 Data Management

Data Registration

As Data Controller, the Trust must register as a Data Controller on the Data Protection Register held by the Information Commissioner. The Academy was first registered on 21/02/12 and is due to renew on 21/02/21

Data Protection Officer

As a public body, Life Academies Trust is required to appoint a Data Protection Officer (DPO).

This DPO role is fulfilled by:

- SBM Ltd

The role of the DPO is to:

- Inform and advise the Trust and its employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact for supervisory authorities.

Data Protection Awareness

In order to ensure organisational compliance, all staff and other key stakeholders (e.g. volunteers) will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee to the organisation or if an individual changes role within the Trust).

Annual data protection refresher training will take place to reinforce the importance of staff adhering to the legislation.

A record of the professional development undertaken by the individual will be retained on their training record.

Data Mapping

LIFE Academies Trust has documented all the data that it collects within a 'Data Flow Map'. This data inventory records:

- the data held

- what the data is used for
- how it is collected
- how consent is obtained
- how the data is stored
- what the retention period is
- who can access the data
- who is accountable for the data
- how the data is shared
- how the data is destroyed

For each data type, the probability of a data breach occurring is assessed (very high, high, medium, low or very low) and actions to be taken to mitigate the risk are recorded.

It is the responsibility of the DPO to ensure the 'Data Flow Map' is kept up to date. The map should be a live document and updated regularly.

3.2 Third Party Suppliers Acting as Data Processors

As Data Controller, the Trust is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all sub-contractors and other third parties in line with the principles of the data protection legislation.

Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the principles of the DPA. These types of agreements include: -

- IT contracts and processes.
- Physical data and hard copy documents.
- Data destruction and hardware renewal and recycling financial and personnel information.
- Pupil and staff records.

Only third-party suppliers who can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners.

The procurement process will ensure that all contracts are suitable and reflect DPA requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract.

The external processor will confirm with the data controller that suitable security and operational measures are in place.

Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the DPA and give contractual assurances.

The DPO may require a specific risk assessment to be undertaken if the data is sensitive, and if an increased risk is likely due to the nature, or proposed nature, of the processing.

A written agreement will be in place between the supplier and the Trust to confirm compliance with the DPA principles and obligations to assist the Trust in the event of data breach or subject access

request, or enquiries from the ICO.

The Trust must have the right conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems.

Any subcontracting must only be done with the written consent of the Trust as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by DPA principles when handling the Trust's data, which shall also include co-operation and eventual secure destruction or return of data.

The school has a 'Third Party Request for Information' form which must be used for third party suppliers acting as a Data Processor for the school.

3.3 Consent

As a Trust we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases, data will only be processed if explicit consent has been obtained.

Consent is defined by the DPA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Privacy Notices

In order to comply with the fair processing requirements of the DPA, the Trust will inform their staff and parents/carers of all pupils of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom their data may be passed, through the use of 'Privacy Notices'.

Privacy notices are available to staff and parents through the following means:

- School website
- School newsletter
- Letter to parents
- Staff Handbook
- Staff Notice Boards

The Use of Pupil Images

Occasionally the Trust may take photographs of its pupils. These images could be used as part of internal displays, printed publications, the school website or our social media accounts.

The Trust will seek consent from all parents/carers to allow the photography of pupils and the subsequent reproduction of these images.

Parents/carers are given the opportunity to opt in. It is not permissible to assume parents/carers are opting in.

Generic consent for all uses of images is not acceptable; parents/carers must give consent to each medium.

Parents must be given the opportunity to withdraw their consent at any time. This should be given in writing to the Academy; however, a verbal withdrawal of consent is also valid and should be reported to the relevant Academy office immediately.

Consent should be recorded on an appropriate Trust school management system (e.g. SIMs)

If images of individual pupils are published, then the name of that child should not be used in the accompanying text or caption unless specific consent has been obtained from the parent/carer prior to publication.

Accurate Data

The Trust will endeavour to ensure that the data it stores is accurate and up to date.

When a pupil or member of staff joins the Trust they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number, NI number for staff), next of kin details, emergency contact and other essential information. At this point, the Trust will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

The Trust will periodically undertake a data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct.

Parents/carers and staff are requested to inform the Trust when their personal information changes.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the Trust will consider each situation on the merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to provide the Academy with written confirmation of withdrawal of consent and specify which areas this is in relation to. (See consent form, appendix 1 on the Trust Social Media and Photography and Use of Images policy).

3.4 Associated Data Protection Policies

- CCTV
- Complaints
- Data Breaches (see appendix 1)
- Records Management
- Subject Access Requests
- Third Party Requests for Information
- Use of Personal Devices

CCTV

The Trust uses closed circuit television (CCTV) images to reduce crime and monitor the Trust buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the Trust property. The Trust has a CCTV policy in place which documents:

- why CCTV is used
- where cameras are sited
- whether covert monitoring is undertaken
- how long images are retained for
- who has access to the images
- the complaints procedure

Complaints

Complaints will be dealt with in accordance with the Trusts Complaints Policy.

Data Breaches – see appendix 1

Privacy Impact Assessments

When considering the purchase of a new service or product that involves processing personal data, a Data Privacy Impact Assessment must be completed by the DPO. If risks are identified as part of the assessment, then appropriate steps to mitigate this risk must be implemented. If these risks are deemed to be 'high risk' then the DPO should consult with the ICO prior to implementation.

The 'Data Privacy Impact Assessment' form must be used for each new service/product.

Records Management

The Trust recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations which will also contribute to the effective overall management of the Trust.

The Trust has a Record Management & Retention policy in place which sets out how it will:

- safely and securely store data (both digital and hard copy data)
- retain data
- dispose of data

Subject Access Requests

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the Trust holds about them and can make a Subject Access Request (SAR).

The Trust has a Subject Access Request policy, which sets out the process that should be followed in the event of receiving a SAR.

Third Party Requests for Information

Occasionally the Trust may receive a request for information on a pupil or member of staff by a third party, such as the police or social services. This would be separate to statutory requests that come through from the DfE or LA, for example, which are covered within the privacy notices.

The Trust has a Third-Party Request for Information policy which sets out the process that should be followed in the event of receiving a third-party request.

Use of Personal Devices

The Trust recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices. The Trust follows the 'Bring Your Own Device' policy which sets out how non-Trust owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members, pupils and visitors to the school.

1. Appendix 1 – Data Breach

Introduction

Although Biggleswade Academy takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen.

Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the Academy

Data Protection Officer (DPO)

The Data Protection Officer is:

SBM Services (UK) Ltd
12 Park Lane Business Centre
Park Lane
Langham
Colchester
CO4 5WR

Email: info@sbmservices.co.uk
Telephone: 01206 671103

Data Compliance Co-ordinators (DCC)

The Data Compliance Co-ordinators are:

Mrs S Spruth – Business Support Manager
Email: sjspruth@biggleswadeacademy.org
Tel: 01767 550616 ex236

Ms C Harrowing – HR Manager
Email: ceharrowing@biggleswadeacademy.org
Tel: 01767 550616 ex258 - Claire

Steps to be taken for Breach

However, the breach has occurred, the following steps should be taken immediately:

1. Internal Notification**:** Individual who has identified the breach has occurred should notify one of the DCC's in the first instance who will then liaise with the DPO. (Individuals may contact DPO direct but unless the breach involves the DCC they should note the Trusts and DPO's preference to channel all breaches via the DCC)

   A record of the breach should be created using the following templates:
   a. Data Breach Incident Form (Appendix A)
   b. Data Breach Log (Appendix B)
   c. Evidence Log (Appendix C)

2. Containment**:** DPO to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. Recovery**:** DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, backup tapes to restore lost or damaged data)

4. Assess the risks**:** Before deciding on the next course of action, DPO to assess the risks associated with the data breach considering the following, which should be recorded in the Data Breach Notification form (Appendix C):

   a. What type of data is involved?
   b. How sensitive is it?
   c. If data has been lost/stolen, are there any protections in place such as encryption?
   d. What has happened to the data?
   e. What could the data tell a third party about the individual?
   f. How many individuals' data have been affected by the breach?
   g. Whose data has been breached?
   h. What harm can come to those individuals?
   i. Are there wider consequences to consider such as reputational loss?

5. Notification to the Information Commissioners Office (ICO): Following the risk assessment in step 4, the DPO should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

   The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

6. Notification to the Individual**:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the academy.

7. Evaluation**:** The DPO should assess whether any changes need to be made to the Academy's processes and procedures to ensure that a similar breach does not occur in the future.

Appendix A – Data Breach Incident Form

Part A: Breach Information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Activity:	

Part B: Breach Risk Assessment

What type of data is involved?	Hard Copy: Yes / No Electronic Data: Yes / No
Is the data categorised as 'sensitive' within one of the following categories?	Racial or ethnic origin: Yes / No Political opinions: Yes / No Religious or philosophical beliefs: Yes / No Trade union membership: Yes / No Data concerning health or sex life and sexual orientation: Yes / No Genetic data: Yes / No Biometric data: Yes / No
Were any protective measures in place to secure the data (e.g. encryption):	Yes / No If yes, please outline:
What has happened to the data?	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	

Whose data has been breached:	
What harm can come to those individuals:	
Are there wider consequences to consider e.g. reputational loss?	

Part C: Breach Notification

Is the breach likely to result in a risk to people's rights and freedoms?
Date ICO notified:
Time ICO notified:
Reported by:
Method used to notify ICO:
Notes:
Is the breach likely to result in a high risk to people's rights and freedoms?
Date individual notified:
Notified by:
Notes:

Part D: Breach Action Plan

Action to be taken to recover the data:	
Relevant trustees to be notified:	Names:
	Date Notified:
Notification to any other relevant external agencies:	External agencies:
	Date Notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	

Appendix B – Data Breach Log

Date Reported:	Notified By:	Reported To:	Description of Breach:	Notification to ICO:	Notification to Individual(s)	Further Actions to be taken:	Reviewed by:
				Yes/No	Yes/No		
				Yes/No	Yes/No		
				Yes/No	Yes/No		

Appendix C – Data Breach Evidence Log

Date:	Description of Evidence:	Details of where evidence is stored/located:	Member of staff who collected data: