DATA PROTECTION POLICY

Policy	**Data Protection Policy**
Policy adopted by Trust Board	**14.6.22**
Reported to LGBs for implementation	**13.7.22**
Implementation Date	**13.7.22**
Review Date	**July 2024**
Policy Source	**SBM Model Policy**

Contents

Part 1 Introduction and Key Definitions

1.1 Introduction

LIFE Education 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 Trust data protection standards — and to comply with the law.

This data protection policy ensures LIFE Education 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 LIFE Education 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 school/academy 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 in 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 Education 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

The Trust will:

- Establish and maintain a positive data protection culture.
- Ensure the Director of Operations prepares a Data Protection policy for approval and adoption by the Finance and Facilities Committee and to 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 that the Trust provides 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.

The Headteachers/ Heads of School will

- Promote a positive data protection culture.
- Ensure that all staff cooperate with the Data Protection policy.
- 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.
- Receive the work of the Data Protection Officer to ensure they are fulfilling their responsibilities.

The Data Protection Officer will:

- Inform and advise the Academy of their obligations under data protection legislation.
- Monitor compliance with the legislation and report to the Finance and Facilities Committee on a termly basis.
- 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 governors.
- Carry out a data protection induction for all staff and keep records of that induction.
- Coordinate the school response to a Subject Access Request.
- Coordinate the school response to a data breach.

Staff at the school will:

- Familiarise themselves and comply with the Data Protection Policy.

- Comply with the Academy data protection arrangements.
- Follow the data breach reporting process.
- Attend data protection training as organised by the school.

Part 3 Detailed Arrangements & Procedures

3.1 Data Management

Data Registration

As Data Controller, the school must register as a Data Controller on the Data Protection Register held by the Information Commissioner. The school was last registered on 19/02/22 and is due to renew on 19/02/23.

Data Protection Officer

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

At LIFE Education Trust the DPO role is fulfilled by:

- SBM Services (UK) Ltd

The role of the DPO is to:

- Inform and advise the school/academy and the 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.
- Coordinate training on data protection for all key stakeholders in the Trust

Data Protection Awareness

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

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 Education Trust has documented all of 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 subcontractors 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 type 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 school to confirm compliance with the DPA principles and obligations to assist the school in the event of a data breach or subject access request, or enquiries from the ICO.

The school 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 school 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 school's data, which shall also include cooperation 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 school 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
- School prospectus
- 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.

Each school in the Trust will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images. Consent will be sought on an annual basis.

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

Generic consent for all uses of images is not acceptable; parents 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 school, however a verbal withdrawal of consent is also valid and should be reported to the Headteacher / Head of School immediately.

Consent should be recorded on 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 prior to publication.

The Academy 'Parental Consent' form should be issued to current parents to seek consent annually.

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

When a pupil or member of staff joins the Academy 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 Academy will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

The school will undertake an annual data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct. This exercise will also provide individuals with the opportunity to review the consent they have given for the Academy to use the information held for internal purposes.

Parents/carers and staff are requested to inform the Academy 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 school will consider each situation on its merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to complete a Withdrawal of Consent form and return this to the Headteacher/Head of School.

3.4 Associated Data Protection Policies

- CCTV
- Complaints
- Data Breaches
- 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 school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school 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
- what the complaints procedure is

Complaints
Complaints will be dealt with in accordance with the Trust Complaints Procedure. An individual may contact the Information Commissioner's Office (ICO) if they are not satisfied with how a complaint has been dealt with by the school. The telephone number for the ICO is 0303 123 1113.

Data Breaches
Although the Trust 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 Trust.

The school has a Data Breach Policy which sets out the process that should be followed in the event of a data breach occurring.

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 school.

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 school/academy holds about them, and can make a Subject Access Request (SAR).

The school 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-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school.

APPENDIX 1

Parental Consent Form

Student Images
Occasionally, we may take photographs of the children at our school. We use these images as part of our school displays and sometimes in other printed publications. We will also use them on our school website, Facebook page and Twitter account.

If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption. If we name a pupil in the text, we will not use a photograph of that child to accompany the article. If a child has won an award and the parent would like the name of their child to accompany their picture we will obtain permission from the parent before using the image.

Learning Journeys and Records of Achievement are used to celebrate your child's progress throughout school. These are sent home at the end of Reception and Year 6. Photographs of individuals, groups or classes of children may appear in these records. *(Amend to reflect the relevant document title and its use or delete if not applicable)*

From time to time, our school may be visited by the media who will take photographs or film footage of a high profile event. Children may appear in these images, which will sometimes be published in local or national newspapers, or on approved websites.

Please use the boxes below to indicate whether you give consent to each medium:

	Yes	**No**
I give permission for my child's photo to be used within school for display purposes	□	□
I give permission for my child's photo to be used in Learning Journey's/Records of Achievement *(amend to reflect relevant document title)*	□	□
I give permission for my child's photo to be used on the school website	□	□
I give permission for my child's photo to be used in other printed publications	□	□
I give permission for my child's photo to be used on the school's social media sites	□	□
I give permission for my child to appear in the media	□	□
I give permission for my child to have a school photograph taken. I understand this printed/digital photograph can be purchased by parents.	□	□

Marketing & Fundraising
We would like to be able to inform you about school based events (such as open mornings, Parent Association fundraising events, class assemblies) either by phone, text, emails or letters.

Please use the boxes below to indicate how you agree for the school to contact you for these purposes (more than one box can be ticked if you consent for more than one medium of communication):

	Yes	**No**
Phone Call:	□	□
Text Message:	□	□
Email:	□	□
Letter:	□	□

Direct Marketing
We would like to be able to inform you about special offers or promotions by certain third parties that might be of interest to you (for example companies offering discounted rates to families during school holiday periods, information about local events) either by phone, text, emails or letters.

Please use the boxes below to indicate how you agree for the school to contact you for these purposes (more than one box can be ticked if you consent for more than one medium of communication):

	Yes	**No**
Phone Call:	□	□
Text Message:	□	□
Email:	□	□
Letter:	□	□

This form is valid for the current academic year. Parental consent for these areas will be requested on an annual basis to ensure that consent is still valid.

Consent to any of the above can be withdrawn by parents. Please provide the school with written confirmation that you withdraw your consent and specify which areas this is in relation to.

Parent/Carer Signature: _____ **Date:** _____

Print Name: _____

Student Name: _____ **Relationship to child:** _____

APPENDIX 2

Staff Consent Form

Staff Images
Occasionally, we may take photographs of the staff employed within our school. We use these images as part of our school displays and sometimes in other printed publications. We also may use them on our school website and social media accounts (e.g. Facebook or Twitter).

Without your consent, we will not use images and videos of you except for legal reasons which we do not require consent for (e.g. staff ID badges).

Learning Journeys and Records of Achievement are used to celebrate our pupil's progress throughout school. These are sent home at the end of Reception and Year 6. Photographs of staff may appear in these records.

From time to time, our school may be visited by the media who will take photographs or film footage of a high-profile event. Staff may appear in these images, which will sometimes be published in local or national newspapers, or on approved websites.

Please use the boxes below to indicate whether you give consent to each medium:

	Yes	**No**
I give permission for my photo to be used within school for display purposes	□	□
I give permission for my photo to be used in Learning Journey's/Records of Achievement	□	□
I give permission for my photo to be used on the school website	□	□
I give permission for my photo to be used in other printed publications	□	□
I give permission for my photo to be used on the school's social media sites	□	□
I give permission for my photo to appear in the media	□	□
I consent to having my photo taken as part of a class or school photograph. I understand this printed/digital photograph can be purchased by parents.	□	□

This form is valid for the length of time you are employed at the school.

Consent to any of the above can be withdrawn at any time. Please provide the school with written confirmation that you withdraw your consent and specify which areas this is in relation to.

Staff Signature: _____

Print Name: _____

Staff Name: _____

Date: _____

APPENDIX 3

Acceptable Use Agreement
For attention of all staff, governors, volunteers, visitors and contractors

Introduction
Our Academy promotes the positive use of technology and assists in developing pupil's knowledge and understanding of digital devices and the internet. We have a duty of care to safeguard pupils when using technology in our Academy. This agreement is designed to ensure that all staff, governors, volunteers, visitors and contractors understand their professional responsibilities when using any form of ICT in our Academy.

Agreement
I understand my role and responsibility in using ICT (including data) and related technologies such as email, the internet and mobile devices at <insert school name / academy>, as detailed below:

1. I will only use the Academy's email/internet/intranet/learning platform and other related technologies for professional purposes or for uses deemed reasonable by the Headteacher or Governing Body.
2. I am aware that all network and internet activity is logged and monitored and can be made available, on request, to the Headteacher in the event of allegations of misconduct.
3. I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, parents or staff on social media or websites in any way which might bring the Academy into disrepute.
4. I will not browse, download or upload or distribute any material that could be considered offensive, illegal discriminatory or copyright infringing.
5. I will only use authorised school social media accounts and Academy approved apps to post information to parents and pupils.
6. I will only use the approved, secure email system(s) for any Academy business.
7. Photographs of staff, pupils and any other members of the Academy community will not be used outside of the internal Academy IT network unless written consent has been granted by the subject of the photograph or their parent/guardian.
8. I will not install software onto the Academy network unless I have received express permission from the Headteacher.
9. I will ensure that personal data is kept secure and is used appropriately, whether on Academy premises, taken off Academy premises or accessed remotely. Personal or sensitive data taken off site must be encrypted and will not be stored on any personal IT equipment.
10. I will not divulge any Academy related passwords and I will comply with Academy IT security procedures.
11. I will ensure that my mobile phone and any other personally owned device is switched off or switched to 'silent' mode when I have directed time with pupils. I will only make or receive calls in specific designated areas such as the staff room.
12. I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to parents or pupils.
13. I will report any incidents of concern regarding pupil's safety to the Academy E-Safety Co-ordinator or the Designated Child Protection Officer.
14. I will support and promote the school's academy's E-Safety and Data Security policies and help pupils be safe and responsible in their use of ICT and related technologies.

Signature: _____ **Date:** _____

Print Name: _____

Role in School: _____

Signature of School Representative: _____ **Date:** _____

Data Breach Process

Contents

Data Breach Process

Although the <school/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 <school/academy>

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

1. **Internal Notification:** Individual who has identified the breach has occurred must notify the <school/academy> DPO. 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, back up 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 giving consideration to 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 <school/academy>.

7. **Evaluation:** The DPO should assess whether any changes need to be made to the <school/academy> processes and procedures to ensure that a similar breach does not occur.

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?	Yes / No If Yes, then the ICO should be notified within 72 hours.
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?	Yes / No If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	

Part D: Breach Action Plan

Action to be taken to recover the data:	
Relevant governors/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:

Subject Access Request

Contents

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

A SAR can be made using the 'Subject Access Request' form (Appendix A).

The DPO has been designated as the person who will coordinate the response to a SAR.

The school is required to provide the individual with the data it holds on them within one calendar month. The school can extend the time to respond by a further two months if the request is complex or they have received a number of requests from the individual. The individual must be contacted within one month of the school receiving their request and explain why the extension is necessary.

The response to the SAR will be provided in an electronic form.

It is permissible to ask the individual who has made the request to be more specific about the information that they require in order to ensure that the information they are provided with meets their requirements rather than providing lots of information that may not be relevant to their query.

Evidence of the identity of the person making the request and their relationship to the pupil must be gained prior to any disclosure of information. This should be recorded on the SAR Log (Appendix B).

Exemptions to a SAR may include:

- Education, Health, Social Work records
- Examination marks and scripts
- Safeguarding records
- Special educational needs
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests e.g. DfE statistical information
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references

For full details of exemptions to a SAR please visit the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

Appendix A
Subject Access Request (SAR) Form
Part A: Data Subject's Details (person whose information you are requesting)

Title:	
Full Name:	
Date of Birth:	
Address:	
Year Group (if pupil at school)	

Part B: Requestor Details

Title:	
Full Name:	
Address:	
Phone Number:	
Email Address:	
Evidence of Identity (e.g. passport, driving license):	Evidence Provided? Yes / No Details:
Status of Requestor:	Data Subject: Yes / No Parent or person with parental responsibility: Yes / No Other: Yes / No If you have selected 'yes' for 'Other', please outline your role here:

Part C: Details of Subject Access Request

Details of Data Being Requested:	

Part D: Declaration

Option i
I , ……., hereby request that Academy provide the data requested about me.

Signed:_____
Date:_____

Option ii

I , ……., hereby request that Academy provide the data requested about ……. (insert child's name) on the basis of the authority that I have.

Signed:_____

Date:_____

Appendix B
Subject Access Request (SAR) Log

Data Subject	Request	Date of SAR	Date DPO notified	ID confirmed	Response Deadline	Extension to Deadline?	Data held by school	Any additional info from requestor?	Any info to be withheld?	Who auth'd with-holding info?	Response checked and approved by DPO
E.g. John Smith	All data held about this staff member	01/02/18	01/02/18	Passport seen 02/02/18	01/03/18	08/03/18: 1 week due to Feb ½ term.	Personnel file – hard copy Email correspondence about individual	JS clarified the request links to a grievance they have with their line manager	Redacted email correspondence to remove reference to other employees	DPO 20/02/18	DPO 01/03/18

Subject Access Request Response

<Trust Letterhead>

<Name>
<Address>

<Date>

Dear <Name>,

Subject Access Request Response

We are responding to your Subject Access Request dated <date> where you requested a copy of all information held and processed by <school name> concerning your child, <name>.

The school has searched the physical records and electronic records that are held in order to respond to your request. *(Examples are included below; please delete from your final copy)*

Response Document Ref. No.	Description of the Data Provided	Purpose of the data processing	Source of the data	Recipients of the data	Period of data storage
1	E.G. Letter to Mrs X dated 22nd October 2019, copied to yourself, regarding pupil x's progress at school and the impact his late arrival has on this.	Public task	Electronic copy stored on school ICT network	Headteacher, Mrs X, Mr X	Retain whilst the child remains at primary school
2	E.G. Attendance summary of pupil x 01/09/2019 to current date.	Public task & legal obligation	SIMS management information system	Capita, Headteacher, Class Teacher, Admin Staff	3 years after the date on which the entry was made
3	E.G. Records of contact from period 6th September 2019 to 4th February 2020 related to pupil x involving school and Mr X.	Public task	Pupil's educational record	Headteacher	Retain whilst the child remains at primary school
4					
5					

6					
7					
8					
9					
10					

The school has not undertaken any automated decision making on the data provided.

The school also holds records of <describe records>; however, these have not been included within the response because <insert basis for excluding the response>.

I hope that this provides a satisfactory response to your request.

Yours sincerely

<insert name>
<insert position>

Third Party Requests for Information Process template

Contents

Third Party Requests for Information
Occasionally the Academy may receive a request for information on a pupil or member of staff by a third party, such as the police or social services.

The police do occasionally ask for personal data as part of an inquiry, but they don't have the automatic right to receive information about our staff or pupils. You should not feel pressured into handing over personal information. There is a special process the police are required to follow to access personal data for certain crime-related purposes.

However, child protection and safeguarding can take priority over data protection. The Children Act 1989 and 2004, Education Act 1996 and 2002 all emphasise the importance of sharing information responsibly where safeguarding is an issue.

Every situation should be assessed on its individual circumstances, and a distinction must be made at this time whether the information has been requested on an emergency basis, (where there is immediate and significant risk to the life and/or limb of a person), or whether the information is required as part of a routine investigation (where there is no immediate threat of harm).

If there is any doubt, then the school's legal advisor should be contacted for advice.

Any decisions about disclosure on safeguarding requirements should be recorded. The member of staff who has disclosed the data should make a record in the pupil or staff file of the following:

- Information that has been disclosed
- Who it has been disclosed to (person, position and agency)
- Who within the school authorised the release of the data
- Date & time of the decision

A 'Third Party Request for Information' form (Appendix A) should be completed for each request which summarises this information.

Appendix A
Third Party Request for Information

This form should be completed where a third party contacts the school requesting that information is shared with them about a member of staff or a student.

Remember, the police and other agencies have processes that they need to follow in order to legitimately gain information that is protected within the Data Protection regulations. However, child protection and safeguarding take priority and if information is requested on an emergency basis where there is immediate or significant risk, information can be disclosed.

This form should be completed on receipt of an information request, with authority sought from the Trust.

A copy should be retained on the relevant staff or pupil file.

Date of Request:	
Time of Request:	
Person receiving request:	
Position:	

Details of Third Party

Name:	
Position:	
Agency:	
How has request been made?	Face to face □ Telephone □ Letter □ Email □ Other (please describe)

Details of Information Requested

Data that has been requested:	
Reason the data has been requested:	

Authorisation to Release Information

Name:	
Position:	
Date:	
Time:	
Authority to release requested information?	Yes / No
Summary of Information to be released:	

Confirmation of Information Released:

Date Information Released:	
Time Information Released:	
Method of Releasing Information:	Face to face □ Telephone □ Letter □ Email □ Other (please describe)
Person who released the information:	
Position:	
Summary of Information Released:	
Follow Up Action to be Taken:	

Each school will have their own CCTV policy in the following format

CCTV Policy template

Contents

CCTV Policy

Introduction

This is the School's approved policy relating to the use of CCTV. <Insert School Name> uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school property.

The system comprises <enter details e.g. a number of fixed and dome cameras.>

The system <does / does not have sound recording capability.>

The CCTV system is owned and operated by <the school / service provider>, the deployment of which is determined by the school's leadership team.

The CCTV is monitored <centrally / remotely> from <where e.g. the school offices> by <insert job description(s)>.

The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the school community.

The school's CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act (DPA). The use of CCTV, and the associated images and any sounds recordings is covered by the DPA. This policy outlines the school's use of CCTV and how it complies with the legislation.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained about their responsibilities under the CCTV policy. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

Statement of Intent

The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use. The Code of Practice is published at:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

CCTV warning signs will be clearly and prominently placed at <insert locations e.g. all external entrances to the school.> Signs will contain details of the purpose for using CCTV (see Appendix A). In areas where CCTV is used, the school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Siting the Cameras

Cameras will be sited so they only capture images relevant to the purposes for which they are installed, (as described above), and care will be taken to ensure that reasonable privacy

expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the legislation.

The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

CCTV will not be used in classrooms but in areas within school that have been identified by staff and pupils as not being easily monitored.

Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

Covert Monitoring

The school may in exceptional circumstances set up covert monitoring. For example:

- Where there is good cause to suspect than an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from a member of the senior leadership team.

Covert monitoring must cease following completion of an investigation.

Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

Storage and Retention of CCTV Images

The school retains CCTV images for <insert length of time school retains CCTV – note that this should be the shortest period you need to meet the original rationale for using CCTV>.

The school stores CCTV images by <insert school process for storing CCTV data – note that storage should be such that it maintains the integrity of the information>.

Access to CCTV Images

Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

Subject Access Requests (SAR)

Individuals have the right to request access to CCTV footage relating to themselves under the GDPR.

All requests should be made in writing using the SAR request form to the <Data Protection Officer/relevant post>. Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified. For example, data, time and location.

The school will respond to requests within 1 calendar month of receiving the request.

The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

Please see the Subject Access Request policy for further details.

Access to and Disclosure of Images to Third Parties

There will be no disclosure of recorded data to third parties other than to authorised personnel, such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators). Requests by third parties should be assessed using the school's Third Party Request for Information policy.

The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Complaints

Complaints will be dealt with in accordance with the <school's/academy's> Complaints Procedure.

Appendix A: CCTV Signage

It is a requirement of the Data Protection Act to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled. The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded.
- The purpose of using CCTV.
- The name of the school.
- The contact telephone number or address for enquiries.