Data Protection Policy

Reviewed: September 2024

Next Review: September 2026

About us

Active Education Sussex Ltd (AES), supports schools to deliver their PE curriculum. It also independently provides wraparound and holiday activities for children.

Whilst providing support to schools, Active Education Sussex is a data processor and the school is the data controller. Active Education Sussex complies with the data protection policies and procedures maintained by the school.

Whilst independently providing wraparound and holiday activities, Active Education Sussex is the data controller. This policy relates to the personal data of staff, pupil and parents that is processed for the provision of these activities.

Contents

1. Aims

AES aims to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
AES is registered with the ICO – Registration number: ZB718683

2. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name, address, email address, contact telephone number • Bank details to enable payment for activities
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Mental and physical health
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3. Roles and responsibilities

This policy sets out the data protection responsibilities of AES. It applies to children and parents accessing services and to **all staff** employed by AES and external organisations, or individuals, working on our behalf. All staff and any other individuals handling personal information on behalf of AES have a responsibility to ensure that they comply with Data Protection legislation and AES policies.

AES ensures that all staff who are involved in processing personal data undertake training as part of their Induction and the organisation provides access to data protection training as part of its Safeguarding responsibilities, via the RSimmonsltd.com website. Staff who do not comply with this policy may face disciplinary action.

3.1 Director

The Director has overall responsibility for ensuring that AES complies with all relevant data protection obligations.

3.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

Active Education Sussex has appointed Roger Simmons as its DPO (rsimmonsltd@gmail.com).

In the event of a query, please contact the Director, Ash Elphick, in the first instance. ashelphick@activeeducationsussex.co.uk or on 07734883068

3.3 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing AES of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - Questions about the operation of this policy
    - Uncertainty about the legal basis for gathering or processing personal data
    - Identification of a data breach

4. Data protection principles

- We will ensure all information collected, processed, shared and stored complies with the principles of GDPR. This means Personal Identifiable Information will be:
- processed lawfully, fairly and in a transparent manner
- collected and used only for the legitimate purpose it was collected
- only collected if required for the legitimate purpose
- accurate and where required, rectified without delay
- kept only as long as it is required
- appropriately secured against unauthorised or unlawful processing, accidental loss, destruction or damage
- processed in accordance with the rights of data subjects
- processed in the European Economic Area unless additional protection has been put in place

5. Legal basis for processing

AES processes staff, child and parent data to meet its contractual obligations when providing employment and a service to the public. The legal basis for processing personal data is detailed below:

- **Legal Obligation** – processing and sharing of staff information to complete safeguarding checks and employment requirements

- **Contract** – processing of personal information for the purpose of an employment contract and the delivery of services purchased by parents for their children

- **Legitimate Interest** – provision of information to parents who have a legitimate interest in knowing about the services available from AES

- **Consent** – where another legal basis is not already in place, such as photographs and videos. Consent is gathered from parents at the start of the contract and can be withdrawn at any time.

6. How long is personal data held

Data retention by AES
Staff data is held for 7 years to enable AES to meet its legal obligations.
Child and parent information is retained until the end of the academic year, before being erased.
Where there is the possibility of the information being required by AES or a parent in the future (such as an accident report), the information will be stored digitally and retained for up to 10 years.

Data retention by AES staff
Staff store lists of children attending activities on their own digital devices to enable the safe delivery of the activities. Upon completion of the activity, any personal data should be uploaded to the AES storage folder, along with any photos or images. Staff are responsible for ensuring all personal data relating to activities is erased from their device at the end of each term.

7. Who is the information shared with

When we share information with others, we make sure it is kept safe and secure, following the requirements set out in law. We share information with organisations so that we can provide the best activities and keep children safe.

Individual data may be shared with:

- catering provider, for the provision of meals
- the providers of educational/ activity software, for the support and improvement of educational standards
- parental communication tools
- Police, emergency services, Social Services and other appropriate professional groups
- Where we transfer personal data to a country or territory outside the UK or European Economic Area, we will do so in accordance with data protection law.

8. How can I access my data

Data protection legislation gives individuals specific rights, which include the right to access their data.
Please see Appendix 1 – Individual Rights Policy and Request Form.

9. Data protection breach

AES will take all preventable steps to hold and process individual data securely. In the unlikely event of a breach, AES has a data breach management process which all staff are aware of and have received appropriate training so they can recognise and react appropriately to a data breach.

All breaches of Data Protection legislation will be reported to the Data Protection Officer who will ensure the process is adhered to and ensure breaches are reported to the ICO where necessary.
Please see Appendix 2 – Breach Management Procedure and Report Form

10. Management of information

AES will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

11. Keeping data safe

Before introducing a new policy, procedure, system or database involving personal data, AES will consider the need for a Data Protection Impact Assessment (DPIA). The DPIA will identify any potential risks of harm to individuals through the misuse of their personal information, allowing these risks to be reduced. A DPIA will be conducted where processing is likely to result in a high risk to individuals.

12. Photographs and videos

As part of AES activities, we may take photographs and record images of individuals within the schools we provide services to. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:
- Within AES notice boards and in AES magazines, brochures, newsletters, etc.
- Online on our Active Education Sussex Ltd website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child.
Please see our Child protection and safeguarding policy for further information.

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must follow the appropriate guidance to keep the information safe
- Passwords that are at least 8 characters long containing letters and numbers are used to access school and AES computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff are not permitted to store individual's personal information on their personal devices beyond the period of the activity. School-owned or Active Education Sussex Ltd Owned equipment (password protected) should be used

(*Please see our online safety policy and acceptable use of technology code of conduct)*

14. Data in transit

All staff and volunteers are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data is protected within the school and when accessed or transported outside the school.

All sensitive and confidential electronic data being taken outside of its normally secure location must be encrypted. All non-electronic data must be transported and stored using an appropriate level of care and security.

Data in transit should be kept to the minimum amount required to safely provide the AES activities to children.

Any data loss must be reported immediately to the Director. Disciplinary action could be taken where staff do not follow the guidance set out in this policy.

15. Training

All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or Active Education Sussex Ltd processes make it necessary.

16. The Regulator

The Information Commissioner's Office is responsible for:

- overseeing compliance with Data Protection legislation
- supporting organisations to become compliant
- enforcing the legal processing of data
- investigating complaints where organisations are not compliant

If you have a concern about the processing of your personal data you should in the first instance contact the Director with your concern. If your concern is unresolved you may make a complaint to the ICO at the following address:

Office of the Information Commissioner
The Information Commissioners, Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF
website: www.ico.gov.uk

Appendix 1 – Individual Rights Policy and Request Form

AES processes the personal data of individuals who have rights under the General Data Protection Regulation 2018. This document sets out the rights of individuals, how the school will support those rights and how an individual can exercise those rights. This document should be read alongside AES's Data Protection Policy.

The individual rights of data subjects are summarised below:

- Right of access – Individuals have the right to access their personal data.
- Right to rectification – Individuals have the right to have inaccurate personal data amended.
- Rights to erasure – Individuals can request that their personal data is deleted where there is no justification for its continued use.
- Right to restrict processing – In the following circumstances an individual can request a temporary restriction of processing activities:
    - whilst AES is establishing the accuracy of data an individual has contested
    - whilst AES is following up any objection raised by an individual
    - when data has been processed unlawfully but the individual wants AES to restrict the processing of it, rather than erase it
    - when the individual needs it in connection with a legal claim
- Right to object – Individuals have the right to object to their information being processed in the following circumstances:
    - If AES has decided processing is necessary either to perform a task in the public interest, as part of its authority, or, as a legitimate interest, and the individual feels this is not applicable
    - If an individual believes there are insufficient grounds for AES to retain information in defence or potential defence of a legal claim
    - If their data is being used for direct marketing purposes
    - If their data is being used for research purposes that do not outweigh the individual's right to privacy

These exceptions only apply in certain circumstances and AES will seek advice from its DPO.

Subject Access Requests

The most common request received for access to personal data. This is called a Subject Access Request. This includes:

- Confirmation that personal data is being processed
- Access to a copy of the data
- The purposes of the data processing

- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for
- The source of the data
- Whether any automated decision-making is being applied to their data

If staff receive a subject access request they must immediately forward it to the Director.

Children and subject access requests

Mature pupils aged 13 and over can make a SAR for themselves. If a pupil is under 13 though, a request must come from their parent or legal guardian.

We expect mature pupils aged 13 or over may make their own requests however a parent or legal guardian may make a request on behalf of their child aged 13 or over if their child is unable to act on their own behalf or gives their consent for the information to be released to the parent.

Responding to a SAR

When responding to requests, AES will:

- ensure the individual has provided appropriate identification
- respond within 1 month of receipt of the request, or 3 months if the request is complex
- provide the information free of charge

Exceptions to the Regulation

AES will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in court in proceedings concerning the child
- Is manifestly unfounded or excessive

Repetitive requests or those asking for further copies of the same information may be considered unfounded or excessive. AES may refuse to act on the request or charge a reasonable fee which takes into account administrative costs.

When AES refuses a request, it will tell the individual why, and tell them they have the right to complain to the Information Commissioners Office.

Individual Rights Request Form

You should complete this form if you want to exercise an individual right afforded under the Data Protection Act 2018, including a Subject Access Request.
*Please fill out the following sections as instructed.

1) **Data subject's details (the person that the data relates to)**

Full name:	
Date of birth:	
Address:	
Phone number:	
Email address:	
Pupil Year group OR staff job role:	

2) **Are you the data subject?**

☐ YES: I am the data subject and I enclose proof of my identity. (Please go to section 4)

☐ NO: I am acting on behalf of the data subject. I will enclose the data subject's written authority and proof of the data subject's identity and my own identity. (Please go to section 3)

2) Requestor details

Full name:	
Address:	
Phone number:	
Email address:	
Relationship to the data subject:	

4**) Individual Right**

Please note you can only select one individual right per form. This request refers to my right:
☐ to access (I want to access information about me)
☐ to rectification (I want to correct information about me)
☐ to erasure (I want to delete data about me)
☐ to restrict processing
☐ to object

5) **Details of request**

(Please give as much information as you can to help with our search such as any relevant dates or names. Being as specific as possible will help us locate your information as quickly as possible.)

In some cases we may consider your request complex if it:

- involves retrieval and appraisal of information from multiple sources
- involves the retrieval of large volumes of information for one data subject which are difficult to separate from information relating to other data subjects
- is one in a series of requests from the same individual
- involves the release of 3rd party data where consent has been refused or cannot be obtained

If we consider your request complex, we can take up to an additional two months to respond. If this is the case, we will let you know within the one month deadline, and as soon as possible.

6) **Proof of Identification (documents supplied as proof of identity or entitlement to request another person's personal data)**

Please list the proof of identification(s) you are providing:	

7) **Declaration**

The completed application form and supporting proof of identity/ entitlement should be emailed or sent to: The Director, Ash Elphick ashelphick@activeeducationsussex.co.uk

Signature of requestor:		Date:	

Appendix 2 – Data Breach Procedure and Report Form

Active Education Sussex Ltd will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow this procedure. When appropriate, our DPO will report the data breach to the ICO within 72 hours.

On finding or causing a breach/potential breach, the staff member must immediately notify the Director.

- The DPO will investigate the report and determine whether a breach has occurred. The DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost, Stolen, Destroyed or Altered
  - Disclosed where it should not have been

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

- The DPO will work out whether the breach must be reported to the ICO. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage, including through:
  - Loss of control over their data or discrimination,
  - Identify theft, fraud or financial loss
  - Damage to reputation or loss of confidentiality
- The DPO will document the decision in the Breach Report Form in case it is challenged at a later date by the ICO or an individual affected by the breach. Breach Reports are stored by AES.

Actions to minimise the impact of data breaches

Staff must take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly high risk or sensitive information.

- Sensitive information being disclosed via email
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the Director as soon as they become aware of the error
- In any cases where the recall is unsuccessful, the Director will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

active education sussex

Breach Management Report

Date breach reported	
Name of person reporting the breach	The person who identified the breach
Member of staff managing the breach	

What breach has occurred (Key facts – use initials rather than names)	What data has been lost or accessed by an unauthorised person
Date the breach occurred	When did it happen
How many individuals does the breach effect	How many people and if a parent, child, staff member or group of people.
What categories of data have been breached	What categories of personal information has been shared and does the breach include sensitive data
What is the likely impact of the breach	This will be the impact of the breach on the data subject(s)
What immediate action has been taken	To contain the breach and prevent it from getting larger
Has the data subject been told of the breach	Have they been contacted already or will they be contacted?
Date DPO advised	Email this completed form to the DPO
DPO recommendation	Including the need to notify the ICO
Date ICO notified	If applicable
Further action required	What additional steps must be taken to reduce the impact of the breach or reduce the risk of repetition. i.e. improvements to procedures or staff training
Date actions completed and breach closed	DPO signs off the breach when actions completed.