



SEIN GDPR Policy

Policy Purpose

This policy is drafted in accordance with the requirements of the UK General Data Protection Regulation ("UK GDPR") UK GDPR and the UK Data Protection Act 2018, 2021 update DPA 2021 update.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any individual and it helps to promote equality across SEIN.

Policy Statement

Everyone has rights regarding the way their personal data is handled. During our activities we will collect, store and process personal data about our service users and others. This makes us a data controller in relation to that personal data.

We are committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

About this Policy

The types of personal data that we may be required to handle include information about service users and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018, 2021 update, and is based on guidance published by the Information Commissioner's Office (ICO). (Collectively 'Data Protection Legislation').

This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.



This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

1. Definitions

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

Personal Data means any information relating to an identified or identifiable, living individual.

This may include the individual's:

- Name (including initials)
- Date of birth
- Identification number
- Location data
- Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data Controllers are the people or organisations who determine the purposes for which, and the way, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. SEIN are the data controller of all personal data used in our business for our own purposes.

Data Users are those of our workforce (including trustees, governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data Processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.

Processing is any activity that involves the use of data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal



data to third parties.

Special Category Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

Workforce includes any individual employed by SEIN such as staff and those who volunteer in any capacity including trustees, members, member of a local governing body, parent helpers and community volunteers.

Data Protection Officer

Emma McCullagh is our DPO and is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

Data Protection Principles

The UK GDPR is based on data protection principles, anyone processing personal data must comply with these principles:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and where necessary kept up to date.
- Kept for no longer than is necessary for the purpose for which it is processed.
- Processed securely using appropriate technical and organisational measures.

Personal Data must also:

- Be processed in line with data subjects' rights.
- Not be transferred to people or organisations situated in other countries without adequate protection.

This policy sets out how SEIN will comply with these principles in relation to any processing of personal data.



Fair and Lawful Processing

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing (see below).
- Whether the personal data will be shared, and if so with whom.
- The period for which the personal data will be held.
- The existence of the data subject's rights in relation to the processing of that personal data
- The right to raise a complaint with the Information Commissioner's Office in relation to any processing.

We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and ensure that we have a lawful basis for any processing.

For personal data to be processed lawfully, it must be processed based on one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

- Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract.
- Where the processing is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011).
- Where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest.
- Where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.
- When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds.
- Where the processing is necessary for employment law purposes, for example in relation to sickness absence.
- Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment.
- Where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities.
- Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.



We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

If any data user is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

Vital Interests

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing.

We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

Where none of the other bases for processing set out above apply then SEIN must seek the consent of the data subject before processing any personal data for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from data subjects. When service users and/or employees and/or volunteers join SEIN a consent form will be required to be completed in relation to them.

This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

Processing for Limited Purposes

Through the nature of our work at times it will be necessary to collect and process personal data. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other agencies or members of our workforce).

We will only process personal data for specific purposes or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.



Accurate Data

- We will ensure that personal data we hold is accurate and kept up to date.
- We will take reasonable steps to destroy or amend inaccurate or out-of-date data.
- Data subjects have a right to have any inaccurate personal data rectified.

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.

Processing in line with data subject's rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any personal data we hold about them.
- Object to the processing of their personal data, including the right to object to direct marketing.
- Have inaccurate or incomplete personal data about them rectified.
- Restrict processing of their personal data.
- Have personal data we hold about them erased.
- Have their personal data transferred.
- Object to the making of decisions about them by automated means.

The Right of Access to Personal Data

Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with SEIN's Subject Access Request Procedure.

The Right to Object

In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking based on a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

An objection to processing does not have to be complied with where SEIN can demonstrate compelling legitimate grounds which override the rights of the data subject.

Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

In respect of direct marketing any objection to processing must be complied with.

SEIN is not however obliged to comply with a request where the personal data is required in



relation to any claim or legal proceedings.

The Right to Rectification

If a data subject informs SEIN that personal data held about them by SEIN is inaccurate or incomplete then we will consider that request and provide a response within one month.

If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the data subject within one month of their request that this is the case.

We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why. In those circumstances we will inform the data subject of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

Data subjects have a right to "block" or suppress the processing of personal data. This means that SEIN can continue to hold the personal data but not do anything else with it.

SEIN must restrict the processing of personal data:

- Where it is in the process of considering a request for personal data to be rectified (see above).
- Where SEIN is in the process of considering an objection to processing by a data subject.
- Where the processing is unlawful but the data subject has asked SEIN not to delete the personal data.
- Where SEIN no longer needs the personal data but the data subject has asked SEIN not to delete the personal data because they need it in relation to a legal claim, including any potential claim against SEIN.

If SEIN has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

Data subjects have a right to have personal data about them held by SEIN erased only in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was originally collected.
- When a data subject withdraws consent – which will apply only where SEIN is relying on



the individuals consent to the processing in the first place.

- When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object.
- Where the processing of the personal data is otherwise unlawful.
- When it is necessary to erase the personal data to comply with a legal obligation.
- If SEIN offers services to a pupil and consent is withdrawn in respect of that pupil in relation to those services.

SEIN is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- To exercise the right of freedom of expression or information.
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law.
- For public health purposes in the public interest.
- For archiving purposes in the public interest, research or statistical purposes.
- In relation to a legal claim.

If SEIN has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

Right to Data Portability

In limited circumstances a data subject has a right to receive their personal data in an electronic readable format, and to have this transferred to other organisation.

If such a request is made then the DPO must be consulted.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

Security procedures

Secure lockable desks and cupboards

Desks and cupboards should be kept locked if they hold confidential information of any kind.

(Personal information is always considered confidential.)



Methods of disposal

Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. In line with SEIN Cyber Security and IT Administration Policy, IT assets must be disposed of in accordance UK GDPR, Waste Electrical and Electronic Equipment Directive (WEEE Directive) and the Information Commissioner's Office guidance on the disposal of IT assets.

Equipment

Data users must ensure that individual monitors do not show confidential information to passers by and that they lock PC's / tablets when left unattended.

Many thanks for all you do and the commitment you show our young people!

Management Signed:

(Emma McCullagh)

01.05.2025