SEAX TRUST

GDPR: Data Protection Policy

SEAX Trust, Registered in England & Wales No 07747149. Registered Office: c/o Grove House School, Sawyers Hall Lane, Brentwood CM15 9DA

This Policy sets out that which will be applied going forward from its adoption

Ratified by SEAX Board of Trustees & Effective Date of Adoption:	**16th October 2024**

Policy Review: Annual
Policy reviewed by the Trust's GDPR Group

Updates October 2024:

Section	Title	Change
2.2	Roles & Responsibilities	Addition stating that annual GDPR training will be undertaken by Trustees
2.2	Roles & Responsibilities	Addition to the role of the Central Team's GDPR lead covering the requirement to provide training
3.1	Data Protection Officer	Change made to cite the Director of HR as the co-ordinator between the DPO and the Trust
3.1	Data Protection Awareness	Addition stating that it is a requirement for Trustees/Governors to undertake annual Cyber Security training.
3.3	The use of images	Staff added to this section, which was previously pupils only
3.4	Associated Data Protection Policies	Confidentiality Agreement, ICT Usage Agreement and paragraph relating to information sharing in an employee medical or mental health emergency added to this section

This Policy is essential reading for all data processors of the SEAX Trust and forms part of the Induction Process for all new staff, volunteers, members of Local Academy Committees, Trustees and Members of the Trust

Contents

Part 1 - Introduction and Key Definitions

1.1 Introduction

SEAX Trust schools need to gather and use certain information about individuals.

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

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

This Data Protection Policy ensures SEAX Trust and its schools:

- comply with data protection law and follow good practice
- protect the rights of pupils, staff, parents/carers and other stakeholders
- remain transparent regarding the storage and processing of individuals' data
- protect themselves from the risks of a data breach

This Data Protection Policy is based on the six principles of the Data Protection Act (DPA) in 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 SEAX Trust and its schools, must collect, handle and store personal information ('data').

'Data' consists of any information that the school/Trust collects and stores about individuals or other 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;
- 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/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, for example, the DfE and certain other organisations, override these rights (this is documented later in the policy under 'Privacy Notices').

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 a curriculum software provider or a payroll provider.

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 SEAX Trust is the 'Data Controller'.

Part 2 - Organisational Arrangements

2.1 Overall Responsibility

SEAX 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

Trustees will:

- Establish and maintain a positive data protection culture
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties
- Ensure the Data Protection Officer prepares a Data Protection Policy for approval and adoption by the SEAX Trust and review and monitor the effectiveness of the Policy; the policy should be reviewed on a regular basis, at least every two years
- 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 each school/location 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
- Attend data protection training as organised by the Executive Team.

The Headteacher will:

- Promote a positive data protection culture
- Ensure that all staff co-operate with the Data Protection Policy
- Ensure that staff are competent to undertake the tasks required of them.
- Coordinate training on data protection for all key stakeholders in the school
- Provide staff with equipment and resources to enable them to protect the data that they are processing
- Carry out a data protection induction for all staff and keep records of that induction
- 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 staff to ensure they are fulfilling their responsibilities

The Data Protection Officer will:

- Inform and advise the SEAX Trust schools of their obligations under data protection legislation
- Monitor compliance with the legislation and report to the Headteacher and SEAX Trust on an annual 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 LAC members

The Trust's GDPR Lead in the Central Team will:

- Act upon information and advice on data protection and circulate to staff and governors/trustees
- Provide data protection induction information for all staff and ensure records are kept of that induction
- Coordinate data protection training for staff and governors/trustees
- Co-ordinate the schools' response to a SAR (with support as required from the DPO)
- Co-ordinate the schools' response to a data breach (with support as required from the DPO)
- Ensure completion of a DPIA for new products or services which involve the processing of data (with support as required from the DPO)

Staff in the Central Team and at the Trust schools will:

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

Part 3 - Detailed Arrangements & Procedures

3.1 Data Management

Data Registration

Schools must register as Data Controllers on the Data Protection Register held by the Information Commissioner. SEAX Trust Schools are registered annually on 1st April each year. New schools joining the trust are added to the register as they join.

Data Protection Officer

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

At SEAX Trust the DPO role is fulfilled by:

- SBM Services (uk) Ltd (a sub-contracted service provider)
- The SEAX Trust Director of HR is the data protection co-ordinator between SEAX and the DPO.

The role of the DPO is to:

- Inform and advise the Central Team, Trust schools 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.

Data Protection Awareness

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

Staff and Governors/Trustees will also be required to complete annual cyber security training to ensure that they are aware of cyber risks and understand the important role that they play in reducing the risk of a successful cyber attack.

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 file.

Data Mapping

SEAX Trust schools have documented all of the data that they collect 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 Data Lead in each school/setting 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 schools are 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 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 data breach or subject access request, or enquiries from the ICO.

The Trust Schools must have the right to 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 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.

The Trust and its schools maintain evidence of the checks that have taken place for each of their third party suppliers.

Third Parties Working on site

There may be times when certain third party individuals undertake work for the Trust, on Trust or school premises (eg therapists, supply staff etc.). Such individuals are often likely to require access to personal data, which may be sensitive in nature, in order to satisfactorily undertake their role. However, they may not have undertaken the usual induction and pre-employment procedures, due to the fact that the Trust is not their direct employer. When and if this is the case, the school must ensure that, at the very least, the individual has completed the following actions before they are given authority to access the data:

- Signed for reading the Trust's Data Protection Policy
- A signed Confidentiality Form must be held
- A written agreement must 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 data breach or subject access request, or enquiries from the ICO
- A pre-employment check must be made, confirming that the individual is a member of their relevant professional body and, therefore, bound by that body's code of conduct.

3.3 Consent

SEAX Trust schools 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 students/young people in certain circumstances, and this will be at the discretion of the Headteacher in conjunction with the parent/carer. Discretion will be on a case-by-case basis and will be dependent on the following factors:

- the child's age (eg likely to be from the age of 13+/when students reach Year 9)
- the child's ability to make an informed decision
- the reason for processing (eg photograph to be displayed in school/school website etc)
- signed agreement between the school and the parent/carer setting out the possible reason(s) for processing to be held by the school in advance

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 (eg 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 any of the following means:

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

Privacy notices will be reviewed regularly.

The Use of Images – Pupil & Staff

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

SEAX Trust schools will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images.

The Trust and its schools will seek consent from all members of staff to allow their photography and the subsequent reproduction of these images.

Consent will be sought on an annual basis.

Parents and staff are given the opportunity to opt in. It is not permissible to assume they are opting in.

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

Parents and staff 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 Data Lead immediately.

Consent should be recorded in the individual school record either in paper form or on the school Management Information System.

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 individual school 'Parental Consent' and 'Staff Consent' forms are used to seek consent when they join the organisation.. The Consent form allows consent for the length of time the individual ~~student~~ attends the school, or works at the Trust, unless/until consent is withdrawn.

Accurate Data

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

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

The school/Trust 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 Trust to use the information held for internal purposes.

Parents/carers and staff are requested to inform the school/s 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 the 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 Data Controller.

3.4 Associated Data Protection Policies

- CCTV — School Policy
- Complaints — SEAX Trust Policy
- Confidentiality Agreement — SEAX Trust Policy
- Data Breaches — SEAX Trust Policy
- Data Privacy Impact Assessments — SEAX Trust Policy
- ICT Usage Agreement — SEAX Trust Policy
- Information sharing in an employee medical or mental health emergency
- Records Management — SEAX Trust Policy
- Subject Access Requests — SEAX Trust Policy
- Third Party Requests for Information — SEAX Trust Policy
- Use of Personal Devices — School Policy
- Remote Working Policy — SEAX Trust Policy
-

CCTV – Site Specific Policy

Some schools use 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. These schools have 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

Complaints – SEAX Policy/Procedure

Complaints regarding Data Protection issues will be dealt with in accordance with the SEAX Trust Complaints Procedure and should be addressed to the SEAX Trust/SEAX Trust school in the first instance. Should the complainant not feel satisfied with the way in which the SEAX Trust/SEAX Trust school deals with their complaint, they can refer the matter to the Information Commissioner's Office (ICO) for further investigation. The telephone number for the ICO is 0303 123 1113.

Confidentiality Agreement

The Trust has a Confidentiality Agreement in place which staff, governors/trustees and volunteers are required to sign on an annual basis. This agreement sets out the expectations the Trust has in relation to maintaining confidentiality.

Data Breaches

Although SEAX 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 Trust data is stored (e.g. a laptop, a USB stick, a mobile phone or a door fob which could allow entry to a third party)
- 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/Trust.

The SEAX Trust has a Data Breach Policy which sets out the process that should be followed in the event of a data breach occurring. However, in all cases/suspected cases of a data breach, staff must report the incident to their GDPR Lead immediately.

Data 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.

It is the duty of each school/site to advise the DPO prior to the purchase of any such product, and to assist in completion of the 'Data Privacy Impact Assessment' process.

ICT Usage Agreements

The Trust has an ICT Usage Agreement in place which staff, governors/trustees and volunteers are required to sign on an annual basis. This agreement sets out the expectations the Trust has in relation to staff safely and securely using the IT network.

Information sharing in an employee medical or mental health emergency

Data protection law allows the Trust to share personal information in an urgent or emergency situation, including to help prevent loss of life or serious physical, emotional or mental harm.

During a medical or mental health emergency where there is risk of serious harm to staff or to others the Trust will share necessary and proportionate information without delay with relevant and appropriate emergency services or health professionals. The Trust may also share necessary and proportionate information with the member of staff's next of kin or emergency contact.

The Trust will use their judgement in each specific situation, sharing only what is necessary and proportionate to the circumstances. The Trust may decide that, whilst it may be necessary and proportionate to provide the emergency services with a full account of the situation, it is only appropriate to provide the member of staff's emergency contact with more limited details.

The Trust staff privacy notice covers this sharing of data. (The Trust may also include links to any other policies that relate to managing staff mental health emergencies).

Records Management – SEAX Policy

The SEAX 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 and Trust schools.

The SEAX Trust has two Record Management & Retention Policies* in place setting out how it will:

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

*The two Policies are:

1. GDPR Record Retention Guidelines – MAIN [IRMS & Groupcall Toolkit for Schools]

2. GDPR Record Retention Guidelines – HR [Juniper Education Guidelines]

Subject Access Requests – SEAX Policy

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).

SEAX 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 – SEAX Policy

Occasionally SEAX Trust and its schools 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.

SEAX 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 – Site Specific Policy

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

Contact Details
SEAX Trust
Grove House School, Sawyers Hall Lane, Brentwood CM15 9DA
Telephone: 01245 963000
Email: admin@seaxtrust.com
Website: www.seaxtrust.com