Data Protection Policy

Document Details	
Category:	Data Protection Policies
Approved By:	Board of Trustees

Ownership

History

Version	

Contents:

Statement of intent

The Sigma Trust is required to keep and process certain information about its staff members, pupils, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation.

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, DfE, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and The Sigma Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012

This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'

This policy operates in conjunction with the following Trust and school policies:

- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
    - Racial or ethnic origin.
    - Political opinions.
    - Religious or philosophical beliefs.
    - Trade union membership.
    - Principles.

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

In accordance with the requirem.024 39osed o71 0 595.32 841.92 reW* nBT/F2 11.04 Tf1 0 0 1 322.01 418

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

3. Accountability

The Sigma Trust will implement appropriate technical and organisational measures to

- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

DPIAs will be used to identify and reduce data protection risks, where appropriate.

4. Data protection officer (DPO)

The Trust will to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection.

A DPO will be appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.

The individual appointed as DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to schools. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to rforming

5. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing

or social care or treatment or management of health or social care systems and services with a basis in law
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law

- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

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.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

The school has privacy notices for the following groups, which outline the information above that is specific to them:

- Prospective employees
- Pupils and their families
- School workforce
- Third parties
- Trustees and governors
- Volunteers

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 may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such ci

- Consent to process a child's data, the school ensures that the requirements outlined in the 'Consent' section are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

6. Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

The Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

When pupils and staff join the Trust, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

7. The right to be informed

Adults and children have the same right to be informed about how the Trust uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO

Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.

All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school will:

- Omit certain elements from the response if another individual's personal data

The Trust has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

11. The right to restrict processing

Individuals, including children, have the right to block or suppress the school's processing of personal data.

The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests

Where the Trust is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Trust reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

12. The right to data portability

Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
-

- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

15. Data protection by design and default

The Trust will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the Trust will ensure that only data that is necessary to achieve its specific purpose will be processed.

The Trust will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
-

- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

17. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Chief Executive Officer will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Where the Trust faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it. Where a breach is likely to result in a risk to the rights and

Where notifying an individual about a breach to their personal data, the Trust will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

The Trust will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR

safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The Trust will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The Trust will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

20.

25. Monitoring and review

This policy is reviewed every two years. The next scheduled review date for this policy is Summer Term 2025