Swanland
Education Trust

Policy for Data Protection (including GDPR)

Document Ref: SET/ADMIN/POL/01-05-18/110

Name and Title of Author:	Chris Huscroft – CEO
Name of Responsible Committee:	Board of Trustees
Trade Union Representative Approval:	N/A
Implementation Date:	May 2018
Review Date:	May 2020
Version:	1
Trustee Approval Date:	May 2018
Target Audience:	All employed staff
Related Documents:	Freedom of information publication scheme E safety policy Child Protection Policy SET Code of Conduct
References:	Data Protection Act 2018 Data Protection Act 1998 https://ico.org.uk/ General Data Protection Regulation Crime Directive https://www.privacyshield.gov/welcome Human Rights Act 1998 Freedom of Information Act 2000

Revision History

Version	Date	Summary of Revision	Revision Author
1	May '18	Trust version created and recommended for approval	CJH

Contents

1. Background

The Data Protection Act 2018 (DPA 2018) makes provision for the General Data Protection Regulation (GDPR) 2016 and the EU Crime Directive 2016 in to UK law. The DPA 2018 replaces the Data Protection Act 1998, superseding the laws developed in compliance with the Data Protection Directive 95/46/EC. The purpose of the updated data protection legislation[1] is to protect the 'rights and freedoms' of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge.

Data protection legislation applies to all data controllers that are established in the UK, who process the personal data of data subjects. It will also apply to data controllers outside of the UK that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the UK.

The Information Commissioner oversees compliance and promotes good practice, regulating all organisations and individuals who process personal data. This Data Protection Policy applies to all personal data held by the Swanland Education Trust, henceforward, known as 'the Trust'.

This policy will be reviewed on a regular basis to ensure that it reflects changes to existing legislation, and any new legislation.

2. Definitions for the Purposes of this Policy

For the purposes of this policy, the following definitions are in relation to Data Protection.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data subject – any living individual who is the subject of personal data held by an organisation.

[1] "The data protection legislation" means–
(a) the GDPR, including the applied GDPR,
(b) DPA 2018, including regulations made under DPA 2018, and
(c) regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive.

Processing – any operation/set of operations performed on personal data or on sets of personal data, whether or not by automated means, 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.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach (PDB) – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the Information Commissioners Office (ICO) and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Child – anyone under the age of 13 years old. The processing of personal data of a child for online services[2] are only lawful if parental or custodian consent has been obtained (this does not include preventive or counselling services). The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Consent – in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

3. Policy Statement

In order to operate effectively, the Trust has to process personal information about people with whom it works. These may include members of the pupils, parents, current, past and prospective employees and suppliers. In addition, it is required by law to process information in order to comply with the requirements of central government.

The Trust is committed to ensuring compliance with data protection legislation. The Trust regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining confidence between the Trust and those with whom it carries out business. The Trust fully endorses the principles of data protection by design and default. To this end, the Trust will ensure its Data Protection Officer is able to fulfil their tasks as defined in data protection legislation.

[2] Refers to information society services as defined by the Electronic Commerce Regulations 2002

Third parties who have access to personal data will be expected to have read and understood this policy. No third party will be able to access personal data without being committed to having obligations no less onerous than the Trust. The Trust will make every effort to ensure data subjects can exercise their rights. Any breach of data protection legislation will be dealt with as a matter of urgency. If required, breaches will be reported to the appropriate authorities and dealt with as criminal offence. The Trust is committed to working with the ICO in all areas relating to personal data.

4. Corporate Requirements

The Trust is a data controller as defined by data protection legislation. It is the responsibility of the Trustees to ensure compliance with Data Protection legislation. However, the Head Teacher is responsible for ensuring compliance within the day to day activities of the school.

All those in managerial or supervisory roles throughout the Trust are responsible for encouraging good information handling practices. Compliance with data protection legislation and this policy is the responsibility of all employees.

Employees are responsible for ensuring that any personal data about them and supplied by them is accurate and up-to-date. All employees who process personal data are responsible for their own compliance with data protection legislation and this policy. Failure to do so may result in disciplinary action which could lead to dismissal.

The Trust's appointed Data protection Officer (DPO) is accountable to the Board of Trustees and will ensure that the tasks outlined within data protection legislation are fulfilled.

The first point of contact for data protection matters is dpo@swanlandeducationtrust.co.uk, however anyone has the right to speak to the DPO about their tasks.

5. Policy Development including Consultation

The following people and groups were consulted in development of this policy:

East Riding of Yorkshire Council *(as part of a traded service);*
IT Governance Ltd as part of the East Riding of Yorkshire Council's traded service *(this document contains material that is distributed under licence from IT Governance Ltd. No reproduction or distribution of this material is allowed outside of your organisation without the permission of IT Governance Ltd.)*

6. Data Protection Principles

All processing of personal data must be conducted in accordance with data protection principles. The Trust's policies and procedures are designed to ensure compliance with these principles.

Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – data protection legislation includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the ICO, outlined on the Trusts records of processing or in line with this Policy.

Personal data must be adequate, relevant and limited to what is necessary for processing

The Trust does not collect information that is not strictly necessary for the purpose for which it is obtained. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the DPO. The DPO will ensure that, on a regular basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

Data that is stored by the Trust must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is the responsibility of the data subject to ensure that data held by the Trust is accurate and up to date. Pupils, parents, employees and suppliers should be required to notify the Trust of any changes in circumstance to enable personal records to be updated accordingly. Processes will be in place to allow for the updating of records. It is the responsibility of the Trust to ensure that any notification regarding change of circumstances is recorded and acted upon.

The DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date. On a regular basis the DPO will review these processes and retention dates for personal data processed by the Trust.

The DPO is responsible for making appropriate arrangements so that, third-party organisations that may have been passed inaccurate or out-of-date personal data are informed, ensuring it is not used to inform decisions about the individuals concerned.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where possible, personal data will be minimised, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the retention schedule and once its retention date is passed, it must be securely destroyed. Any data retention that exceeds the retention period must be approved by the Head Teacher. They must ensure that the justification is clearly identified and in line with the requirements of data protection legislation.

Personal data must be processed in a manner that ensures the appropriate security

The Trust will carry out risk assessments taking into account how state of the art technical measures are, the costs of implementation and the risk/likelihood to individuals if a security breach occurs, the effect of any security breach on the Trust itself, and any likely reputational damage including the possible loss of customer trust.

Both the Trust (as controller) and its processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including where appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

Data protection legislation includes provisions that promote accountability and governance. These complement the transparency requirements. This accountability additional principle requires the Trust to demonstrate that it complies with the principles and states explicitly that this is the Trust responsibility.

The Trust demonstrates this compliance through this policy, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, and establishing formal procedures in relation to data protection.

7. Data Subjects' Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.

- To request the ICO assess whether any provision of the data protection legislation has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller (ported).
- To object to any automated profiling that is occurring without consent.

The Trust makes every effort to ensure that data subjects may exercise these rights. A data subject may make a data access request as described in Appendix 3, Subject Access Requests. These requests are under normal circumstances free of charge and will be dealt with in one month (although they can be extended by two months in some circumstances).

Personal data must not be disclosed about a third party except in accordance with data protection legislation. If it appears absolutely necessary to disclose information about a third party, advice should be sought from the DPO.

Data subjects also have the right to complain to the Trust in relation to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled. This will be done in line with the Trust's Policy for Complaints.

Disclosure of data

The Trust ensures that personal data is not disclosed to unauthorised third parties which includes family members, friends, suppliers, government bodies and other public sector organisations. All employees should exercise caution when asked to disclose personal data held on another individual to a third party.

All requests to provide data must be supported by the appropriate documentation. Data protection legislation permits disclosures for a number of reasons without consent, these include:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party; and
- to protect the vital interests of the individual, this refers to life and death situations.

It is the responsibility of employees to ensure that they have the authority to share information and that the recipient is authorised to receive such information. Failure to do so could lead to action under the Trust's disciplinary procedure (and, in exceptional circumstances, criminal charges).

Advice should always be sought from the DPO if there is any uncertainty around the disclosure of information.

8. Data Transfers

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate 'level of protection for the fundamental rights of the data subjects'.

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

- An adequacy decision.
- Privacy shield.
- Binding corporate rules.
- Model contract clauses.

Exceptions, in the absence of the above a transfer of personal data to a third country or international organisation, shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

9. Consent

The Trust understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be valid.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The data controller must be able to demonstrate that consent was obtained for the processing operation. For special categories data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Where the Trust provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

Whether or not a photograph needs to be protected or falls under data protection legislation can be open to interpretation and the quality of the photograph. However, the school takes this matter extremely seriously and seeks to obtain parents' consent for the use of photographs outside the school and, in particular, to record their wishes if they do not want photographs to be taken of their children.

Processors and Contracts

The Trust will ensure that any processor it engages have a written contract or agreement in place. This is important so both parties understand their responsibilities and liabilities. Processors must only ever act on

documented instructions. To be compliant with data protection legislation contracts must include specific items.

Retention and Disposal of Data

The Trust will not keep personal data in a form that permits identification of data subjects for longer than is necessary, in relation to the purpose(s) for which it was originally collected. It may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Trust's retention schedules.

Personal data must be disposed of securely in accordance with data protection principle 6. Appropriate procedures must be followed when disposing of personal information. The Trust will ensure that secure disposal methods are available to staff.

10.Data Inventory

The Trust has established an Information Asset Register which help determine the flow of data through the organisation. The Trust is aware of any risks associated with the processing of particular types of personal data and the level of risk to individuals associated with the processing of their personal data.

11.Impact Assessments

The Trust will implement technical and organisational measures to ensure that by default, personal data is processed were necessary. Data protection impact assessments (DPIAs) will be carried out in relation to the processing of personal data, and in relation to processing undertaken by other organisations on behalf of the Trust.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, presents a risk to the rights and freedoms of an individual, the Trust, prior to the processing, will carry out a DPIA. A single DPIA may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA, it is clear that the Trust is about to commence processing of personal data that could cause damage and/or distress to the data subjects, or is deemed high risk (including to the reputation of the Trust), the DPIA must be escalated for review to the DPO. The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

12.Incidents and Breaches

The Trust will always treat any data protection incident/breach as a serious issue. In the event of a breach, or suspected breach (incident), the DPO must be informed immediately.

An investigation will take place in line with the Trust's procedures. This includes Human Resources to ensure any disciplinary action is taken if deemed appropriate and Legal Services. The point of contact for the ICO is the DPO.

The Trust has an obligation to report certain data protection breaches to the ICO within 72 hours of the Trust being made aware. The DPO will notify the ICO following an assessment of the breach. If required, the DPO will also arrange for the affected data subjects to be notified. Any data processors the Trust is working with are also required to report data protection breaches to the ICO, as well as cooperate with the ICO to resolve the issue. Data processors must also notify the Trust of any breach which affects the Trust's personal information, within the 72 hour window.

The ICO has the authority to sanction significant financial penalties of up to €20 million or 4% of global turnover (fines in the UK will be based on the current exchange rate). Data processors also hold liability for data protection breaches.

The Trust recognises data subjects' right to compensation if they have suffered material or non-material damage as a result of an infringement of data protection legislation. Any claim for compensation will be dealt with through the Trust's normal procedures.

13. Training

It is the Trust's policy that all employees and processors who have access to the Trust's personal data receive the appropriate training, in order to comply with data protection legislation. The Trust will accordingly ensure that data protection training is available for staff.

Training in data protection matters should be provided before any access to personal data is permitted, and mandatory refresher training should be undertaken at intervals thereafter to maintain awareness.

Data protection training is a crucial element of staff awareness. All individuals need to be aware of their obligations relating to any personal data they process as part of their Trust duties. Failure to adhere to this policy can result in serious misconduct and lead to the prosecution of employees.

14. Outcomes and Impacts

- Prevent the inappropriate use of personal data held by the Trust.
- Ensure employees are aware of their responsibilities for handling personal data and that failure to do so could result in disciplinary proceedings and in some cases criminal proceedings.
- Ensure services and employees know who to contact for advice.
- Training requirements are identified and staff have the required level of data protection knowledge.
- Uphold data subjects' rights.
- Data processors working on behalf of the Trust are aware of their responsibilities and handle personal data in accordance with this policy.
- The Trust has an appointed DPO and his duties are defined.
- The Trust is compliant with data protection legislation.