Data Protection Policy

Equalities Statement

Over recent years, schools and academies have (in line with other institutions and public bodies) been working towards an improved understanding of the diverse nature of their communities. Much of the work is in response to new legislation that places an increased duty on schools, academies and other settings to tackle radicalisation and to establish a positive ethos of British Values. Legislation requires schools and academies both to eliminate direct or indirect discrimination, victimisation or harassment and to promote equalities for students, staff and others who use their facilities.

In our Trust we work to ensure that there is equality of opportunity for all members of our community who hold a range of protected characteristics as defined by the Equality Act 2010, as well as having regard to other factors which have the potential to cause inequality, such as, socio-economic factors.

Document Management	
Approved by:	Board of Directors
Approved on:	17 July 2018
Review Date:	Term 6 2021
Responsibility for review:	Chief Operating Officer

1) Data Protection Statement

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) are the law that protects personal privacy and upholds individual's rights. They apply to anyone who handles or has access to people's personal data.

2) Policy Objectives

This policy is in place to ensure all staff, directors and governors are aware of their responsibilities and outlines how Swale Academies Trust (The Trust) complies with the core principles of the GDPR. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

The Trust as the Data Controller will comply with its obligations under the GDPR and DPA. The Trust is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

3) Applicable Data

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Personal information also includes an identifier such as a name, an identification number, IP address, location data or an online identifier.

4) The Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

5) Transfer Limitation

Personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

6) Lawful Basis for processing personal information

The appropriate lawful basis (or bases) must be established and documented when processing any personal data.

- **Public Interest** - 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 school
- **Contractual** - Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- **Legal Obligation** - Processing is necessary for compliance with a legal obligation to which the data controller is subject
- **Vital Interests** - Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- **Legitimate Interests** - Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party
- **Consent** - The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent from be kept separate from those other matters

  Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

7) Sensitive Personal Information

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
    (a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
    (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
    (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
    (e) the processing relates to personal data which are manifestly made public by the data subject
    (f) the processing is necessary for the establishment, exercise or defence of legal claims
    (g) the processing is necessary for reasons of substantial public interest
    (h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
    (i) the processing is necessary for reasons of public interest in the area of public health.

Unless the Trust can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

8) Data Protection Impact Assessments (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the Chief Operating Officer (COO) for support and guidance and once complete, the COO will refer the finalised document to the DPO for sign off.

9) Documentation and records

Written records of processing activities must be kept, records of processing will be maintained.

The Trust will conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

10) Privacy Notices

The Trust will issue privacy notices as required, informing data subjects about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why the Trust will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

The Trust will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11) Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

12) Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

13) Data Retention

The Trust maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Schools must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the schedule. This includes requiring third parties to delete such data where applicable.

14) Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The Trust expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules, law and Acceptable Use Policy on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies)
- not remove personal information, or devices containing personal information from the school's premises unless appropriate security measures are in place to secure the

information and the device (School owned and encrypted devices or Trust issued Google Drive)

- not store personal information on local drives, private devices, USB drives, removable storage, private cloud storage or private (personal) email accounts
- staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure
- staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA

15) Information Security

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's Acceptable Usage Policy.

The Trust will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

The Trust will only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Where external organisations are used to process personal information on behalf of the Trust, additional security arrangements will be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- Sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the COO.

16) Data Security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data containing personal information is encrypted or password-protected on a local hard drive of a school owned device and backed up on network area. Personal information stored on a network area must be restricted via security groups and backed up. Personal information can be stored on the Trust Google Drive as long as access is known as restricted.

Data must not be saved on removable storage (memory sticks and removable drives).

All electronic devices are password-protected or encrypted to protect data loss.

Staff, directors and governors must not use their personal email accounts for trust purposes.

If sensitive or confidential information is being sent by email the details should be contained in a password protected document.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. Avoid circular emails where possible.

Before sharing data, all staff members will ensure:

- They are allowed to share it
- That adequate security is in place to protect it.
- The recipient has been outlined in a privacy notice.

The security of storage systems, and access to them, should be reviewed on an annual basis.

17) Data Breaches

Staff should ensure they inform their Data Protection Lead immediately that a data breach is discovered and make all reasonable efforts to recover the information.

The DPO must be informed and they will report the data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals.

The affected individuals must be notified if the breach is likely to result in a high risk to their rights and freedoms.

Swale Academies Trust takes its duties under the GDPR seriously and any data breach disclosure may result in disciplinary action.

18) Training

The School will ensure that staff are adequately trained regarding their data protection responsibilities.

19) Consequences of a Failure to Comply

Any failure, by staff, to comply with any part of this policy may lead to disciplinary action under the Trust's disciplinary procedures and this action may result in dismissal for gross misconduct.

If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

20) Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.