SENTAMU ACADEMY LEARNING TRUST
PART OF THE DIOCESE OF YORK EDUCATIONAL TRUST
INSPIRE ALL

Data Protection Policy

May 2018

Approved by Sentamu Academy Learning Trust Board of Directors on 16th July 2018

Next review due May 2019

SALT Vision Statement:

"Be Extraordinary"

Mission Statement:

We believe that young people achieve their fullest potential when they have a vision of everything their lives could become. The Bible (John 10:10) quotes Jesus as saying, "I have come that they may have life and may have it in all its fullness". As academies, we commit ourselves to inspiring our students, and equipping them with the resilience and determination to unlock their unique gifts and realise their highest aspirations. We aim to achieve this through following distinctively Christian principles, and focusing on four key areas, service, achievement, leadership and teamwork.

Contents

1. Aims

The Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • 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.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics

	• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The Trust and each of its Academies process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by the Trust, all Members, Directors, Governors and to external organisations or individuals working on our behalf including voluneers. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust board

The Trust board has overall responsibility for ensuring that the Trust and each of its academies comply with all relevant data protection obligations supported by the Local governing Committee and Principal/Head teacher of each Academy.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Trust board and, where relevant, report to the board their advice and recommendations on Academy data protection issues.

Academy Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Emma Brice and is contactable via Brice.E2@sentamuacademy.org She is supported by an Information Governance Service provider and Data Protection Representatives (DPR) at each Academy to manage the day to day operation of the regulations. See appendix 3.

The DPR is the first point of contact for individuals whose data the academy processes, and for the ICO.

5.3 Chief Executive/Principals/Data Protection Representatives

The Chief Executive, Principals/Head teachers and Data protection representatives act as the representative of the data controller on a day-to-day basis.

5.4 All staff (including Members, Directors, Governors and volunteers) and others

Staff and others are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy Trust of any changes to their personal data, such as a change of address (where applicable)
- Contacting the DPR/DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that the Trust must comply with.

The principles say that personal data must be:

- 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 purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Academy's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests (SARs) must be submitted in writing, either by letter, or email to the DPO. A person acting on behalf of a data subject must provide his or her own name and contact details, as well as those of the data subject. In all cases, SARs must be made using the form App 2, and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.1 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils age 12 or over may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request, with the exception of the summer holidays; during this time, all reasonable efforts will be made to respond within one month.
- Will provide the information free of charge

- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time (where consent is required)
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. Such requests should be made in writing, addressed to the Trust's Data Protection Officer Emma Brice, via the following email: Brice.E2@sentamuacademy.org

11. CCTV

SALT uses CCTV in various locations around some of its Academies to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV. CCTV policies will be in place on the Academies where it exists.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Trust's Data Protection Officer Emma Brice, via the following email: Brice.E2@sentamuacademy.org

12. Photographs and videos

As part of the Trust's activities, we may take photographs and record images of individuals within our Trust.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within each Academy on notice boards and in Academy magazines, brochures, newsletters, etc.
- Outside of each Academy by external agencies such as the Academy photographer, newspapers, campaigns
- Online on Academy or Trust websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a DPO, a suitably qualified Information Governance Service and Data Protection Representatives, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Academies and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Portable electronic devices, such as laptops and mobile phones that contain, or have access to, personal data are password / pin protected to avoid unauthorised use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access. Confidential waste will be shredded.
- Where personal information needs to be taken off site, staff must sign it in and out from the Academy office
- Passwords that are at least 8 characters long containing letters and numbers are used to access Academy computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Staff are not permitted to use portable hard-drives or USB sticks to transfer information between home and the Academy, unless specific permission to do so has been given in writing from either the Trust's Data Protection Officer or the Chief Operating Officer.
- Staff, pupils, directors or governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment (see our ICT acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. We will either shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The Academy will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an Academy context may include, but are not limited to:

- A non-anonymised dataset being published on the Academy website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a Academy laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Academy's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect the Trust's practice. Otherwise, or from then on, this policy will be reviewed annually for the first two years, and thereafter **every 2 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information policy and publication scheme
- E-safety Policy
- Acceptable IT Use Policy
- Records Management Policy
- CCTV Policy (where appropriate)
- Data Retention Schedule
- Child Protection Policy
- Information Protective Marking and Handling Policy

Appendix 1 - Information Security and Data Breach Procedure

We must keep our information safe. This is particularly true of the personal information we hold about our pupils, their families, our employees and third parties. However, all our data is important and this procedure applies to any confidential information including details about finance and banking, security arrangements, business matters, contracts and procurement processes.

It is important that our employees understand what to do in the event that something goes wrong and our information is put at risk. All employees must report any known or possible incidents where information or the files/systems containing them has:

- been lost or stolen;
- been sent or disclosed to another party in error;
- been sent without adequate security protection or safeguards;
- been accessed by someone who does not have permission to do so (including our staff and pupils);
- become unavailable for an extended period due to problems with our computers or IT network;
- become unavailable due to fire, flood or other problems with our buildings;
- been the target of any attempt to 'hack' our computer systems, including malicious emails;
- been the target of any attempt to gain access to information by deception (this is known as 'blagging');
- been processed in any way that breaches the Data Protection Policy or other policies governing how Sentamu Academy Learning Trust manages its information.

Incident Response

Where somebody may be at immediate risk of harm a senior member of academy staff must be informed **immediately** and all reasonable steps must be taken to warn the individual(s) without delay. In such circumstances consideration should also be given to contacting the Police.

In the event or any known or suspected breach of information security the following steps must be taken –

1. The staff member, Director, Governor or volunteer who identifies the breach must notify the Data Protection Representative, Chief Executive Officer and Principal/ Head Teacher or a Deputy Head teacher/Vice Principal immediately. If the incident is discovered outside the academy's opening hours it must be reported as soon as it reopens. If an incident is considered particularly serious, (for example if someone may be at risk of physical harm or lots of records have been compromised) the incident should be reported immediately by contacting Brice.E2@sentamuacademy.org.

2. The staff member handling the incident (the DPO/DPR, Principal/Head teacher or their nominated deputy) must -

    a. Establish whether information is still being put at risk. If so steps must be taken to secure it immediately - for example contact the IT Supplier to shut down a compromised system or arrange for a security company to board up a door or window.
    b. Decide if, when and how any individuals affected by the incident will be notified and what advice they should be provided with.
    c. Where possible, and safe to do so, attempt to recover lost or stolen information or equipment.
    d. Report any criminal activity and lost or stolen property to the Police.
    e. Have academy staff immediately change any passwords or access codes that may have been compromised and warn them if they might expect phishing emails or other malware to be sent to them.

f. Notify the Chief Executive Officer, Principal/Head Teacher, Chair of Directors and Chair of Governors in a timely fashion, they should be informed quickly about more serious incidents.

g. Where the information could aid fraudulent activity, consider the need to notify banks or companies and organisations we work with.

h. Take any steps to recover data from back-ups or copies held elsewhere.

i. Consider any possible impact on the running of the Academy, take steps to inform any affected parties and mitigate the impact upon them.

j. If the incident may be newsworthy, consider the need to take media relations advice, for example from the Diocesan Public Relations Officer.

k. Where very sensitive personal data, or large volumes of less sensitive personal data, has been compromised it may be appropriate to report the breach to the Information Commissioner's Office (ICO). From May 2018 serious incidents must be reported within 72 hours. Guidance is available on the ico.org.uk website or on the ICO telephone helpline.

l. Keep records that will demonstrate what has happened and assist an investigation into what went wrong.

The Information Governance Team will help with response to data breach and information security incidents. They can be contacted for advice on (01482) 613295 or 613378, or information@hullcc.gov.uk

Staff should note that it is **not** the policy of Sentamu Academy Learning Trust to pursue serious disciplinary measures against staff who make genuine human errors but any failure to report or attempt to hide an information security incident will be dealt with extremely seriously.

Investigation

Once the initial response to the incident has taken place it is important that the full circumstances are properly investigated. This should be done promptly to ensure that any ongoing risks can be identified and addressed.

The investigation should be undertaken by a staff member nominated by the Principal/Head Teacher; this can be the person who dealt with the initial incident response.

The investigation should include consideration of the following –

1. What data was compromised, including numbers of records and their sensitivity.
2. What happened, where appropriate including a chronology of events.
3. Review existing safeguards and procedures, how effective they were and any additional measures that could be put in place.
4. Known or potential adverse impacts on data subjects and any advice or support that should be provided to them.
5. Any breaches of policy or procedure and how these should be addressed.
6. Any HR or disciplinary action that may be necessary.
7. Costs and any likely financial implications for the Trust.
8. Potential for any ongoing illegal or unauthorised use of the data.
9. Consideration of any issues with partners or suppliers.
10. Regulatory issues and whether the matter was reported to the ICO.
11. Any Data Protection Act offences relating to knowingly or recklessly obtaining or disclosing personal data that may need to be reported to ICO or the Police.

Appendix 2 - Data Protection Representatives

Academy	Contact Details
Archbishop Sentamu Academy	Tel 01482 781912 Rikki Barnett – Data Manager, Vicky Moore – e-Safety Co-ordinator Mandy Watson, Director of HR (Staff data)
Aspire Academy	Chris Mulqueen, Principal Tel 01482 318789
Newland St John's CE Academy	Jo Langcaster – Business Manager Tel: 01482 305740
St James CE Academy	Sue Daddy – Business Manager Tel: 01482 825091
Information Governance Service (SALT staff only)	01482 613295 or 613378 or information@hullcc.gov.uk