Adopted:	**July 2020**
Next review:	**July 2022**
Approved by:	**NSAT Trust Board**
Responsibility:	**Data & Compliance Director**

Northern Star Academies Trust
Information Policy

Contents

1. Statement of intent

Northern Star Academies Trust is required to keep and process certain information about its employees, pupils, SCITT trainees, governors, trustees, volunteers, applicants and other people the Trust has a relationship with in accordance with its legal obligations under the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The Trust may, from time to time, be required to share personal information about its staff, pupils or individuals with other organisations, mainly the Local Authority (LA), other schools and educational bodies.

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

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

2. Legal framework

2.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

2.2. This policy will be implemented in conjunction with the following other Trust policies:

- Information Security Policy
- Freedom of Information Policy
- Surveillance and CCTV Policy
- Acceptable Use Policy – Pupils
- Acceptable Use Policy - Staff

3. Applicable data

3.1. The Information Policy applies to information in all forms, including but not limited to: -

- Hard copy or documents printed or written on paper
- Information or stored electronically, including scanned images
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer or an online applications
- Information or data stored on or transferred to removeable media such as CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops
- Speech, voice recordings and verbal communications, including voicemail
- Video recordings / online recording of any type of meeting, including lessons
- Published web content, for example intranet and internet
- Photographs and other digital images

3.2. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address.

4. Data Protection

Personal data will be processed in accordance with the requirements of GDPR and in compliance with the data protection principles specified in the legislation.

4.1. Northern Star Academies Trust has notified the Information Commissioner's Office that it is a data controller.

4.2. The Trust has appointed a Data Protection Officer (DPO). Details of the DPO can be found here:

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to Trustees / governors on the above matters

4.3. The Data & Compliance Director is the specific point of contact (SPOC) for the Trust. Duties will include: -

- Ensuring that there are centralised Trust wide processes and procedures relating to data protection and information management
- Internal quality assurance across the Trust for Data Protection
- Communication on best practice relating to Data Protection for the Trust
- Specific point of contact for the Trust schools for Data Protection

4.4. Headteachers are the Senior Information Risk Officer with each school. They will be supported by a Data Protection Champion for the administration of Data Protection in the school. Each school has the responsibility to ensure that Trust policies and procedures are adhered to.

5. Information Asset Register (IAR)

5.1. The DPO will advise the Trust in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- The owner of that asset;
- Description and purpose of the asset;
- Types of data
- Format and location of the asset;
- Who has routine access to the information;
- Who we share this information with,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset
- General description of security measures
- Type of disposal required and disposal method

5.2. The IAR will be reviewed on an annual basis by the asset owners. If there are any significant changes to the assets, the Data & Compliance Director and Data Protection Officer will be informed of any these changes to information assets.

6. Information Asset Owners (IAO)

6.1. An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. Information Asset Owners will be defined by each school and detailed in the Information Asset Register.

6.2. IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

7. Training

7.1. The Trust will provide a training schedule for Data Protection Training as well as a template for each school on which to record when employees have completed an information governance / data protection training module and when a refresher is due to be completed. Each school is responsible for maintaining this record.

7.2. The Data & Compliance Director will ensure that appropriate guidance and training material is provided to each school and, if necessary, liaise with the DPO with regards to this. Schools will ensure that this is delivered to the relevant staff, governors and other authorised users, including how to access information on procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

7.3. If the Trust or school employs any third-party contractors who have access to personal information of individuals, they will ensure that adequate training in data protection and information governance has been provided.

8. Privacy notices

8.1. The Trust will provide privacy notices for schools.

8.2. The Trust and school will provide a copy or a link to the online privacy notice to data subjects each time it obtains personal information from or about that data subjects. This includes to pupils and parents at the start of their time at the school.

8.3. The main privacy notice will be displayed on the Trust and each school's website in an easily accessible area.

8.4. A privacy notice for employees will be provided at commencement of their employment with the Trust or school.

8.5. A privacy notice for Trustees and Governors will be provided at the commencement of their term of office with the Trust or school.

8.6. Annual data checking of key personal information is undertaken for pupils, employees, trustees and governors. A link to the privacy notice will also be provided.

8.7. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. CCTV, volunteers, school trips, projects).

8.8. Privacy notices will be signed off by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's Information Asset Register.

9. Information sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for the school to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (as above). Any ad-hoc sharing of information will be done in compliance with our legislative requirements.

9.1. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it by using the approved Trust procedure.
- Who will receive the data has been outlined in a privacy notice.

9.2. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust or School containing sensitive information are supervised at all times.

9.3. The physical security of the Trust or Academy within the Trust's buildings and storage systems, and access to them, is reviewed as part of the whole school review risk register. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

9.4. Northern Star Academies Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Headteacher of each school is responsible for continuity and recovery measures are in place to ensure the security of protected data.

10. Data Protection Impact Assessments (DPIAs)

10.1. The Trust or school within the Trust will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks. This will allow the identification and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust or Academy within the Trust's reputation which might otherwise occur.

10.2. This must be at the start of a project or before new software / systems / applications which process personal data are implemented. If the type of processing changes for an already implemented piece or software / system / application then the information asset owner will liaise with the Data Protection Champion / Headteacher to ascertain if a new DPIA needs to be conducted or updated.

10.3. The Data Protection Champion or Headteacher will use the documentation in the centralised GDPR area to complete a DPIA and inform the Data & Compliance Director. If the school is unsure whether a DPIA is required then contact the Data & Compliance Director.

10.4. All DPIAs must be signed off by the DPO.

11. Retention periods

11.1. Retention periods will be determined by any legal requirement, best practice or national guidance, and the organisational necessity to retain the information. In addition, IAOs will consider the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

11.2. The Trust has opted to adopt the retention schedule suggested by the Information and Records Management Society (IRMS). See Appendix 1.

11.3. Some educational records relating to former pupils or employees of the Trust or Academy within the Trust may be kept for an extended period for legal reasons.

12. Destruction of records

12.1. Retention periods for records are recorded in the school's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include appropriate shredders and confidential waste bins.

12.2. Advice in regards to the secure destruction of electronic media will be sought from relevant IT support.

12.3. The Trust will provide a destruction log which will be based on the IRMS toolkit to log the date of disposal.

13. Third party Data Processors

13.1. All third-party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained. This will be logged in the electronic log of contracts.

13.2. Relevant senior leadership may insist that any data processing by a third party ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

14. Access to Information – Subject Access Requests (SAR)

14.1. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. Requests under this legislation should be made to the Headteacher within each school.

14.2. Any member of staff/governor/trustee may receive a request for an individual's personal information. Whilst GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged on the school SAR log by the Data Protection Champion within the school and acknowledged within 5 days.

14.3. The school will consult the procedures for handling a SAR and if necessary speak to the Data & Compliance Director. If the request is complex, advice will be sought from the DPO.

14.4. We must be satisfied as to your identity and may have to ask for additional information such as:

- Valid Photo ID (driver's licence, passport etc);
- Proof of Address (Utility bill, council tax letter etc);
- further information for the school to be satisfied of the applicant's identity;

14.5. Only once the school is satisfied of the requestor's identity and has sufficient information on which to respond to the request will it be considered valid. We will then respond to your request within the statutory timescale of one calendar month.

14.6. A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

14.7. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

14.8. The school can apply a discretionary extension of up a further 2 calendar months to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. The Trust or School will seek guidance from the DPO if it wishes to apply an extension, the and information the applicant within the first calendar month of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases The Trust or School may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply. A fee may be charged for complex request a reasonable fee will be charged which will be based on the administrative cost of providing the information.

14.9. For secondary settings only: If a subject access request is made by a parent whose child is 12 years of age or over we may seek consent from the child to share their information or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

14.10. Requests received from parents asking for information held within the pupil's Education Record will be dealt with under a Subject Access Request as the Trust is not a maintained school.

15. Access to Information – Freedom of Information Request

15.1. Please refer to the Freedom of Information Request Policy.

16. Data Subject Rights

16.1. As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR including:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to the Data Protection Champion / Headteacher of the school who will acknowledge the request and respond within one calendar month. Advice regarding such requests may be sought from the Data & Compliance Director or DPO.

16.2. 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.

16.3. Where personal data has been made public within an online environment, the Trust or Academy within the Trust (whichever is relevant) will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

17. Information Breach

17.1. Please refer to the Information Security Policy and procedures.

17.2. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

18. Protecting Biometric Information

18.1. There is a statutory requirement to have a policy in place where the Trust or school processes Special Category Biometric data. This currently only applies to secondary schools within the Trust and the following points detail the nature of this processing, including what information is processed and for what purposes. This is included in the Trust's privacy notices.

18.2. Northern Star Academies Trust will comply with the additional requirements of sections 26 to 26 of the Protections of Freedoms Act 2012, this includes provisions which relate to the use of biometric data in schools and colleges who use an automated biometric recognition system. These provisions are in addition to the requirements of GDPR.

18.3. Biometric data is defined as personal data relating to the physical, physiological or behavioural characteristic of an individual which allows the identification of that individual. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

18.4. An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual. For example, where a fingerprint is used to identify an individual and allow them access to an account.

18.5. Biometric Data is defined in the GDPR 2018 and the Data Protection Act 2018 as a special category of personal data, and it therefore requires additional measures to be put in place in order to process it, as detailed below.

19. Processing of Biometric Information

19.1. *'Processing'* of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- Storing pupils' biometric information on a database system; or
- Using that data as part of an electronic process**,** for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

- Any processing of Biometric data will only be carried out where there is a lawful purpose for the processing, as defined under Article 6 and Article 9 (Schedule 1) of the GDPR 2018. The purposes will be outlined in the Trust's privacy notices which will be made available to the relevant individuals.

20. Consent for the Processing of Biometric Information

20.1. The school processing the biometric information will ensure that it has obtained explicit consent to process the biometric information from the pupil and both of their parents / carers and members of staff (where relevant). They will be informed of the Trust's intention to process the individual's biometric data. This will be carried out through readily available privacy notices and communications, prior to or at the point of obtaining consent, and will include:

- The type of biometric data
- What it will be used for
- The parent's and pupil's rights to withdraw or refuse consent
- What the alternative arrangement will be if consent is refuse or withdrawn

20.2. Under no circumstances will the Trust or school collect or process the biometric data of an individual without their explicit consent or the consent of at least one authorised parent/carer, this will be obtained prior to obtaining any biometric data. If one parent objects in writing, then the Trust or school will not be permitted to take or use that child's biometric data.

All consent must be freely-given, specific, informed and unambiguous, and will be obtained through a clear affirmative action. This will be obtained through the new admissions data collection forms and staff data collection forms. This is consent is also checked on an annual basis for pupils and staff as part of the data checking process.

20.3. Where the Trust or school collects additional Biometric data, or begins to process the biometric data for a new purpose, new consent must be gained to ensure that the individual or their parent/carer is fully informed. This consent must also meet all of the standards outlined in this section.

20.4. If a pupil is using biometric software for their own personal purposes (e.g. facial recognition technology) this is classed as private use not processing by the Trust or school, even if the software is accessed using school or college equipment.

21. Length of Consent and Withdrawing Consent

21.1. The Biometric data will be securely destroyed if consent is withdrawn or if the Trust's retention period is reached.

21.2. Consent can be withdrawn at any time by the parent/carer or the individual, by contacting the Data Protection Champion within each school.

21.3. If a student under the age of 18 objects to the processing of their Biometric data, this will override the consent of the parents/carers and processing will not continue under any circumstances.

22. Alternative to Biometric Data

22.1. The school will ensure that where consent is refused or withdrawn there is an alternative solution which does not require the obtaining or processing of Biometric data. This will ensure that the consent is freely given and that no pressure is placed on the individual or their parent/carer to consent in order to take part in the Trust's or school's processes.

23. Data Protection Impact Assessment for Biometric Information

23.1. Where a new system involving Biometric data, or a new form of processing for Biometric data is introduced, the school will ensure that they have completed a Data Protection Impact Assessment (DPIA) to address any risks associated with the project prior to the implementation of the project.

24. Quality Assurance

24.1. The DPO will carry out periodic reviews of Information Governance practice. The Data & Compliance Director will oversee the implementation of recommendations across the Trust made as a result of the reviews.

24.2. The Data & Compliance Director will agree, on an annual basis, an area of Information Governance as part the Trust's internal scrutiny and assurance processes.