

David Nieper

ACADEMY

Data Protection Policy and Privacy Notice

This policy was updated by Joy Williams, Business Manager and Reviewed by Anthony Gribben-Lisle, Data Protection Officer (DPO)

Version Control

Version 1	Approved February 2018
Version 2 (updated after GDPR)	Reapproved Autumn 2018
Version 3	Re approved Autumn 2019
Fully revised Version 4	Reapproved Spring 2021

Signed:	Date:

Due for review Spring 2022

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions	3
4. The Data Controller.....	4
5. The Data Protection Officer.....	4
6. Data protection principles.....	4
7. Roles and responsibilities	5
8. Privacy/Fair Processing Notice	5
9. Subject access requests	6
10. Images and Recordings	7
11. Data Protection Impact Assessments.....	7
12. Parental requests to see the educational record	8
13. Automated Decision Making and Profiling.....	8
14. Storage of records	8
15. International transfers	8
16. Disposal of records	9
17. Training.....	9
18. Monitoring arrangements	9
19. Links with other policies	9

1. Aims

Our academy aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 2018 and the requirements of the General Data Protection Regulation (GDPR) (2018).

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

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 2018 and is based on [guidance published by the Information Commissioner's Office](#) and [model privacy notices published by the Department for Education](#).

It also takes into account the provisions of the [General Data Protection Regulation](#), legislation which came into force in 2018.

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.

This policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: <ul style="list-style-type: none">• Contact details• Racial or ethnic origin• Political opinions• Religious beliefs, or beliefs of a similar nature• Where a person is a member of a trade union• Physical and mental health• Sexual orientation• Whether a person has committed, or is alleged to have committed, an offence• Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed

Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, who processes the data on behalf of the data controller
Data Protection Officer	A person, other than the data controller if they are a person, who oversees the data protection strategy of an organisation and its implementation to ensure compliance with GDPR requirements

4. The Data Controller

Our academy processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our academy delegates the responsibility for data for students and their parents to the Assistant Headteacher – Curriculum and Data. The HR Officer (PA to Headteacher) has responsibility for personal data relating to staff. Information relating to visitors is monitored by the Receptionist.

The academy is registered as a data controller with the Information Commissioner’s Office and renews this registration annually.

5. The Data Protection Officer

As required by all Public Bodies, the Academy has appointed a Data Protection Officer (DPO) to oversee all aspects of this Policy and associated Procedures and Codes of Practice. Details of their name and contact details will be published on the Academy website as well as being available to all staff as required.

6. Data protection principles

The Data Protection Act is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

7. Roles and responsibilities

The Board of Trustees has overall responsibility for ensuring that the academy complies with its obligations under the Data Protection Act.

Day-to-day responsibilities rest with the headteacher, or the Business Manager in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

Students and their parents are responsible for providing the academy with relevant personal details and ensuring that they inform the academy of any changes to their personal data.

Visitors are responsible for providing correct information to the academy at the time of their visit and they must comply with the visitor policy at all times whilst on academy property.

8. Privacy/Fair Processing Notice

8.1 Students and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the academy is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

Once our pupils reach the age of 13, we are legally required to pass on certain information to Derbyshire County Council, which has responsibilities in relation to the education or training of 13-19-year-olds. Parents, or pupils if aged 16 or over, can request that only their name, address and date of birth be passed to Derbyshire County Council by informing the SIMS, Data and IT Officer via email or in writing within 6 months of their child's 13th birthday.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

For further information please see our Privacy Notice on our website (under the Academy Policies tab)

8.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our academy. The purpose of processing this data is to assist in the running of the academy, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies

- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the PA to the Headteacher.

Please see the document "School Guidelines on Records Retention Periods" for further guidance on how long records need to be retained by the academy.

For further information please see our Privacy Notice on our website (under the Academy Policies tab)

8.3 Visitors and Other Stakeholders

We process data relating to visitors and other stakeholders who come to the academy. The purpose of processing this data is to ensure the safety and wellbeing of the students and staff in our care as well as for health and safety purposes in the event of an emergency evacuation. This data includes, but is not limited to, information such as:

- Name
- Company representing
- Name of person visiting
- Purpose of visit
- DBS number if applicable
- Car registration number
- Photograph

This information is retained in our visitor entry system for a period of two months and then it is automatically deleted by the system. Access to the system is restricted to authorised users only and is password protected.

For further information please see our Privacy Notice on our website (under the Academy Policies tab)

9. Subject access requests

Under the Data Protection Act, individuals have a right to request access to information the academy holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The person's name and the nature of any association with the academy (e.g. student, staff member, parent)
- A correspondence address

- A contact number and email address
- Details about the information requested

The academy will not reveal the following information in response to subject access requests:

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

If a subject access request does not relate to the educational record, we will respond within 30 calendar days.

10. Images and Recordings

- 10.1 Where the academy collects images and/or recordings and individuals may be identified in those images, arrangements for collection, storage and disposal will be carefully considered based on the basis for processing. In some cases, arrangements, for example for the security or sharing of media may differ from standard procedures. In particular, the academy will;
 - 10.2 Ensure that all images collected for marketing and communications purposes are supported by clear and informed consent, which may be amended or withdrawn by the individual at any time. The academy will ensure that those who give consent are aware of the limitations of their right to restrict processing in relation to images already published in digital or paper form, and seek to involve individuals in the approval process for any use of their image which might have a significant public reach or impact
 - 10.3 Ensure that CCTV images and recordings are collected, stored and used within a secure environment, in accordance with the published procedures and codes of conduct
 - 10.4 Use images and recordings created as part of the teaching, learning and assessment process to provide access and support to pupils as part of their learning programme. This may include the recording of lessons and other activities, which may include images of teachers, pupils and other staff.
 - 10.5 Images and recordings of staff, created for the purposes of delivering teaching, learning and assessment through online platforms, or to create reusable teaching and learning resources, will be separately classified and subject to specific criteria for retention and re-use.

11.Data Protection Impact Assessments

- 11.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the academy is planning to use a new form of technology), we will, before commencing the processing, carry out a Data Protection Impact Assessment (DPIA) to assess:
 - 11.1.1 whether the processing is necessary and proportionate in relation to its purpose;
 - 11.1.2 the risks to individuals; and
 - 11.1.3 what measures can be put in place to address those risks and protect personal data.

12. Parental requests to see the educational record

Parents of pupils at this academy do not have an automatic right to access their child's educational record. The academy will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

13. Automated Decision Making and Profiling

Any Automated Decision Making or Profiling which the Academy carries out can only be done once the Data Controller and DPO are confident that it is complying with Data Protection Laws. If Staff therefore wish to carry out any Automated Decision Making or Profiling, they must inform the Data Controller who will coordinate the completion of a comprehensive DPIA to evaluate the risks associated with the proposed processing activities. Staff must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

14. Storage of records

- Paper-based records that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Personal information should not be routinely saved on portable electronic devices, laptops or other removable media.
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from reception
- Passwords that are at least 12 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Use of USB devices is restricted within the academy. If permission is given by the Headteacher encryption software is used to protect all portable devices and removable media.
- Staff, or governors who store personal information on their personal devices are expected to follow the same security procedures for academy-owned equipment and to make their device available for inspection and removal of any personal data on leaving the employment / service of the academy.

15. International transfers

15.1 The academy may transfer personal data outside the United Kingdom, including to the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway), on the basis that such countries are designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards (e.g. by way of binding corporate rules or standard data protection clauses) or where we obtain the relevant data subjects' explicit consent to such transfers. Staff must not export any Personal Data outside the UK without the approval of the Data Protection Officer.

15.2 We will inform data subjects of any envisaged international transfers in our privacy notices.

16. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

17. Training

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

Staff will then receive yearly training and will be updated during the year as necessary via staff briefings or email.

18. Monitoring arrangements

The Business Manager is responsible for monitoring and reviewing this policy with the DPO.

The SIMS, Data and IT officer checks that the school complies with this policy by, among other things, reviewing school records on a termly basis.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every year**.

At every review, the policy will be shared with the governing board.

19. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme. It also links to the Safeguarding Policy, the Visitor Policy, the CCTV Policy and the Health and Safety Policy as well as the School Guidelines on Records Retention Periods issued by Derbyshire County Council.