SOUTH LINCOLNSHIRE ACADEMIES TRUST (SLAT)

# United Kingdom General Data Protection Regulation

## Including Privacy Notices for Staff and Students

Aspire - Challenge – Achieve

| Author | Link | Date Approved |
|---|---|---|
| Chief Operating Officer | Chief Executive Officer | Jan - 26 |
| **Policy Type** | **Date of Next Review** | **Approved By** |
| Trust | Jan - 27 | Trust Board of Directors |

South Lincolnshire Academies Trust

## 1.0 Introduction

This Policy sets out the obligations of South Lincolnshire Academies Trust ("the Trust") regarding data protection and the rights of staff, students, parents, suppliers and Governors ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

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

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out must be followed at all times by the Trust, its employees, agents, contractors, or other parties working on behalf of the Trust.

The Trust is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

## 2.0 The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1.1.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;

2.1.1.2 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;

2.1.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

2.1.1.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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

2.1.1.6 Regulation in order to safeguard the rights and freedoms of the data subject; 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.

## 3.0 Lawful, Fair, and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

3.1.1.1 the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

3.1.1.2 processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

3.1.1.3 processing is necessary for compliance with a legal obligation to which the controller is subject;

3.1.1.4 processing is necessary to protect the vital interests of the data subject or of another natural person;

3.1.1.5 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 controller;

3.1.1.6 processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

## 4.0 Processed for Specified, Explicit and Legitimate Purposes

4.1.1 The Trust collects and processes the personal data set out in Appendix A of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us)

4.1.2 The Trust only processes personal data for the specific purposes set out in Appendix A of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

## 5.0 Adequate, Relevant and Limited Data Processing

The Trust will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

## 6.0 Accuracy of Data and Keeping Data Up To Date

The Trust shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

## 7.0 Timely Processing

The Trust shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

## 8.0 Secure Processing

The Trust shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 20 and 21 of this Policy.

## 9.0 Accountability

9.1.1 The Trust Data Protection Officer is the Chief Operating Officer of South Lincolnshire Academies Trust, 01778 422365.

9.1.2 The Trust shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

9.1.2.1 The name and details of the Trust, its data protection officer, and any applicable third-party data controllers;

9.1.2.2 The purposes for which the Trust processes personal data;

9.1.2.3 Details of the categories of personal data collected, held, and processed by the Trust; and the categories of data subject to which that personal data relates;

9.1.2.4 Details (and categories) of any third parties that will receive personal data from the Trust;

9.1.2.5 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

9.1.2.6 Details of how long personal data will be retained by the Trust; and

9.1.2.7 Detailed descriptions of all technical and organisational measures taken by the Trust to ensure the security of personal data.

## 10.0 Privacy Impact Assessments

The Trust shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Trust's data protection officer and shall address the following areas of importance:

10.1.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

10.1.2 Details of the legitimate interests being pursued by the Trust;

10.1.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

10.1.4 An assessment of the risks posed to individual data subjects; and

10.1.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

## 11.0 The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

11.1.1.1 The right to be informed;

11.1.1.2 The right of access;

11.1.1.3 The right to rectification;

11.1.1.4 The right to erasure (also known as the 'right to be forgotten');

11.1.1.5 The right to restrict processing;

11.1.1.6 The right to data portability;

11.1.1.7 The right to object;

11.1.1.8 Rights with respect to automated decision-making and profiling.

## 12.0 Keeping Data Subjects Informed

12.1.1 The Trust shall ensure that the following information is provided to every data subject when personal data is collected:

12.1.1.1 Details of the Trust including, but not limited to, the identity of Mr Alex Roffe, Data Protection Officer;

12.1.1.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Appendix A of this Policy) and the legal basis justifying that collection and processing;

12.1.1.3 Where applicable, the legitimate interests upon which the Trust is justifying its collection and processing of the personal data;

12.1.1.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.1.1.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.1.1.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers);

12.1.1.7 Details of the length of time the personal data will be held by the Trust (or, where there is no predetermined period, details of how that length of time will be determined);

12.1.1.8 Details of the data subject's rights under the Regulation;

12.1.1.9 Details of the data subject's right to withdraw their consent to the Trust's processing of their personal data at any time;

12.1.1.10 Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

12.1.1.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

12.1.1.12 Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.1.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.1.2.1.1 Where the personal data is obtained from the data subject directly, at the time of collection;

12.1.2.1.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

12.1.2.1.2.1 If the personal data is used to communicate with the data subject, at the time of the first communication; or

12.1.2.1.2.2 If the personal data is to be disclosed to another party, before the personal data is disclosed; or

12.1.2.1.2.3 In any event, not more than one month after the time at which the Trust obtains the personal data.

## 13.0 Data Subject Access

13.1.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Trust holds about them. The Trust is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

13.1.2 All subject access requests received must be forwarded to Mr Alex Roffe, the Trust Data Protection officer. South Lincolnshire Academies Trust, Edinburgh Crescent, Bourne, Lincs PE10 9DT.

13.1.3 The Trust does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

## 14.0 Rectification of Personal Data

14.1.1 If a data subject informs the Trust that personal data held by the Trust is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.1.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

## 15.0 Erasure of Personal Data

15.1.1 Data subjects may request that the Trust erases the personal data it holds about them in the following circumstances:

15.1.1.1 It is no longer necessary for the Trust to hold that personal data with respect to the purpose for which it was originally collected or processed;

15.1.1.2 The data subject wishes to withdraw their consent to the Trust holding and processing their personal data;

15.1.1.3 The data subject objects to the Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);

15.1.1.4 The personal data has been processed unlawfully;

15.1.1.5 The personal data needs to be erased in order for the Trust to comply with a particular legal obligation.

15.1.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

15.1.2 Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and

in such cases the data subject shall be informed of the need for the extension).

15.1.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

## 16.0 Restriction of Personal Data Processing

16.1.1 Data subjects may request that the Trust ceases processing the personal data it holds about them. If a data subject makes such a request, the Trust shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.1.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## 17.0 Data Portability

17.1.1 The Trust passes personal data using automated means to third parties including Show My Homework, Doodle and SAM learning. The data is then used by the Trust staff for the purposed of teaching and learning. Data is not used solely to make automated decisions.

17.1.2 Where data subjects have given their consent to the Trust to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Trust and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

17.1.3 To facilitate the right of data portability, the Trust shall make available all applicable personal data to data subjects in the following formats:

17.1.3.1 Electronic PDF or

17.1.3.2 paper copies

17.1.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.

17.1.5 All requests for copies of personal data shall be complied with within one month of the data subject's request this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension.

## 18.0 Objections to Personal Data Processing

18.1.1 Data subjects have the right to object to the Trust processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling).

18.1.2 Where a data subject objects to the Trust processing their personal data based on its legitimate interests, the Trust shall cease such processing forthwith, unless it can be demonstrated that the Trust's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

## 19.0 Personal Data

The personal data that may be collected, held, and processed by the Trust is listed in Appendix A.

## 20.0 Data Protection Measures

The Trust shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

20.1.1.1 The e-mail system is password protected.

20.1.1.2 Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies will be shredded, and electronic copies will be deleted securely.

20.1.1.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

20.1.1.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

20.1.1.5 Emails should be deleted when they no longer serve a purpose for their original intention. All temporary files associated therewith should also be deleted; *There may be a need for Pastoral staff to keep e-mails to ensure continuity of care. These will only be kept on the school's secure e-mail system.* Emails will not be included in Subject Access Requests unless they have been retained.

20.1.1.6 Facsimile transmission will not normally be used to send information. Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

20.1.1.7 Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using recorded delivery.

20.1.1.8 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Trust requires access to any personal data that they do not already have access to, such access should be formally requested from the DPO.

20.1.1.9 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

20.1.1.10 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Trust or not, without the authorisation of the Executive Head Teacher or the DPO.

20.1.1.11 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

20.1.1.12 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

20.1.1.13 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Trust or otherwise without the formal written approval of the Chief Executive Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary. All mobile devices to be locked using a secure password.

20.1.1.14 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Trust where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Trust that all suitable technical and organisational measures have been taken);

20.1.1.15 All personal data stored electronically should be backed up and backups stored offsite. All backups will

be encrypted.

20.1.1.16 All electronic copies of personal data should be stored securely using passwords;

20.1.1.17 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

20.1.1.18 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Trust, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

## 21.0 Organisational Measures

The Trust shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

21.1.1.1 All employees, agents, contractors, or other parties working on behalf of the Trust shall be made fully aware of both their individual responsibilities and the Trust's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

21.1.1.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Trust that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Trust;

21.1.1.3 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately trained to do so;

21.1.1.4 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately supervised;

21.1.1.5 Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

21.1.1.6 The performance of those employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be regularly evaluated and reviewed;

21.1.1.7 All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

21.1.1.8 All agents, contractors, or other parties working on behalf of the Trust handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Trust arising out of this Policy and the Regulation;

21.1.1.9 Where any agent, contractor or other party working on behalf of the Trust handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Trust against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

21.1.1.10 CCTV footage will not normally be included in a Subject Access Request where it is not possible to isolate the requester's image without identifying other individuals, unless those individuals have consented or it is reasonable to provide the footage following appropriate redaction.

## 22.0 Data Breach Notification

22.1.1 All personal data breaches must be reported immediately to the Trust's data protection officer.

22.1.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

22.1.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 22.4) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

22.1.4 Data breach notifications shall include the following information:

22.1.4.1 The categories and approximate number of data subjects concerned;

22.1.4.2 The categories and approximate number of personal data records concerned;

22.1.4.3 The name and contact details of the Trust's data protection officer (or other contact point where more information can be obtained);

22.1.4.4 The likely consequences of the breach;

22.1.4.5 Details of the measures taken, or proposed to be taken, by the Trust to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

# Appendix A Privacy Notice – School Staff

## How we use your information

### The categories of information that we collect, process, hold and share include:

- Personal information (such as name, address, date of birth, employee or teacher number, National Insurance number)
- Special categories of data including characteristics information such as gender, age, ethnic group
- Contract information (such as start dates, hours worked, post, roles and salary information)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Relevant medical information
- Information necessary for payroll

### Why we collect and use this information

We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid

### The lawful basis on which we process this information

We process this information under **Departmental Censuses in the Education Act 1996 – this information can be found in the guide documents on the following website** https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information. Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with Data Protection Legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this at the time of collection.

Storing this information **We hold school workforce data for seven years after you have left employment with the academy.**

### Who we share this information with

- our local authority
- the Department for Education (DfE)
- our payroll provider

### Why we share school workforce information.

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

We are required to share your information with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

## Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.
The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
To contact the department: https://www.gov.uk/contact-dfe

## Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, please contact the school directly.
You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

## Further information:

If you would like to discuss anything in this privacy notice, please contact:

Mr A Roffe, Data Protection Officer, South Lincolnshire Academies Trust, Edinburgh Crescent, Bourne, Lincolnshire. PE10 9DT, 01778 422365

## Appendix B. Privacy Notice- Students How we use your information in School

### Why do we collect and use pupil information?

We collect and use your pupil information under Article 6 EU UK-GDPR 1. (c) as it is a legal requirement to go to school and we need this information to run the school and comply with laws.

We use your data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

### The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- Special educational needs information
- Information on your behaviour including exclusions

### Collecting pupil information

Most of the pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

### Storing pupil data

We hold pupil data usually until you are 25 but qualification information only for 2 years after they have gained that qualification and SEN or incident information until you are 30 years old

### Who do we share your information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- Aged 14+ The Learning Records Service
- 13-19 year olds information shared with youth support service
- For more information about services for young people, please visit our local authority website.
- Learning Packages e.g. Doddle, GCSE Podcast

## Why we share pupil information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

## Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mr A Roffe, the Data Protection Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

## Contact: For more information and detail please see the SLAT web site.

If you would like to discuss anything in this privacy notice, please contact:

Mr A Roffe, Data Protection Officer, South Lincolnshire Academies Trust, Edinburgh Crescent, Bourne, Lincolnshire. PE10 9DT, 01778 422365