



DATA PROTECTION AND GDPR AND PRIVACY STATEMENT

Last Review	October 2020
Next Review Date	October 2021

Policy statement

1.

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as an organisation we will collect, store and **process personal data** about our pupils, **workforce**, parents, service users and others. This makes us a **data controller** in relation to that **personal data**.

1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.4 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2. About this policy

2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, service users and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the [Data Protection Act 2018], and other regulations (together '**Data Protection Legislation**').

2.2 This policy and any other documents referred to in it set out the basis on which we will **process any personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3. Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

4. Data Protection Officer

4.1 As a trust we are required to appoint a Data Protection Officer (“DPO”). Our DPO is Naomi Fearon and they can be contacted at;

Take 1 Studios, Gregory Boulevard, Nottingham, NG7 6BE

naomi@take1studios.co.uk or 0115 9708982

4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.3 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

5. Data protection principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

5.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

5.1.3 Adequate, relevant and not excessive for the purpose;

5.1.4 Accurate and up to date;

5.1.6 Not kept for any longer than is necessary for the purpose; and

5.1.6 **Processed** securely using appropriate technical and organisational measures.

5.2 **Personal Data** must also:

5.2.2 Be **processed** in line with **data subjects'** rights;

5.2.2 Not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing of personal data** by the Take 1.

6. Fair and lawful processing

6.1 Data Protection Legislation is not intended to prevent the **processing of personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

- 6.2.1 that the **personal data** is being **processed**;
- 6.2.2 why the **personal data** is being **processed**;
- 6.2.3 what the lawful basis is for that **processing** (see below);
- 6.2.4 whether the **personal data** will be shared, and if so with whom; the period for which the **personal data** will be held;
- 6.2.5 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- 6.2.6 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

6.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

6.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

6.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011);

6.4.3 where the law otherwise allows us to **process the personal data** or we are carrying out a task in the public interest; and

6.4.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data**.

6.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

6.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;

6.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

6.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

6.5.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

6.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

6.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

6.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.9 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

6.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

6.11 When pupils, service users and or our Workforce join Take 1 a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

6.12 In relation to all pupils and service users under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.

6.13 We will generally seek consent directly from a pupil who has reached the age of 13, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

6.14 If consent is required for any other **processing of personal data** of any **data subject** then the form of this consent must:

6.14.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

6.14.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

6.14.3 Inform the **data subject** of how they can withdraw their consent.

6.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

6.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

6.17 A record must always be kept of any consent, including how it was obtained and when.

7. Processing for limited purposes

7.1 In the course of our activities as an organisation we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils, service users or members of our **workforce**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

8. Notifying data subjects

8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

8.1.1 our identity and contact details as **Data Controller** and those of the DPO;

8.1.2 the purpose or purposes and legal basis for which we intend to **process that personal data**;

8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;

8.1.4 whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;

8.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy;

8.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and

8.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

9. Adequate, relevant and non-excessive processing

9.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

10. Accurate data

10.1 We will ensure that **personal data** we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11. Timely processing

11.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

12 Processing in line with data subject's rights

12.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

- 12.1.1 request access to any **personal data** we hold about them;
- 12.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;
- 12.1.3 have inaccurate or incomplete **personal data** about them rectified;
- 12.1.4 restrict **processing** of their **personal data**;
- 12.1.5 have **personal data** we hold about them erased
- 12.1.6 have their **personal data** transferred; and
- 12.1.7 object to the making of decisions about them by automated means.

The Right of Access to Personal Data

12.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure.

The Right to Object

12.3 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

12.4 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

12.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

12.6 In respect of direct marketing any objection to **processing** must be complied with.

12.7 Take 1 is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

12.8 If a **data subject** informs the Take 1 that **personal data** held about them by the Take 1 is inaccurate or incomplete then we will consider that request and provide a response within one month.

12.9 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.

12.10 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

12.11 **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the Raleigh Learning Trust can continue to hold the **personal data** but not do anything else with it.

12.12 Take 1 must restrict the **processing** of **personal data**:

12.12.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);

12.12.2 Where the Take 1 is in the process of considering an objection to processing by a **data subject**;

12.12.3 Where the **processing** is unlawful but the **data subject** has asked Take 1 not to delete the **personal data**; and

12.12.4 Where the Take 1 no longer needs the **personal data** but the **data subject** has asked the Take 1 not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Take 1

12.13 If Take 1 has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

12.14 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

12.15 **Data subjects** have a right to have **personal data** about them held by Take 1 erased only in the following circumstances:

12.15.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;

12.15.2 When a **data subject** withdraws consent – which will apply only where the Take 1 is relying on the individuals consent to the **processing** in the first place;

12.15.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;

12.15.4 Where the **processing** of the **personal data** is otherwise unlawful;

12.15.5 When it is necessary to erase the **personal data** to comply with a legal obligation; and

12.16 Take 1 is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

12.16.1 To exercise the right of freedom of expression or information;

12.16.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

12.16.3 For public health purposes in the public interest;

12.16.4 For archiving purposes in the public interest, research or statistical purposes; or

12.16.5 In relation to a legal claim.

12.17 If Take 1 has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

12.18 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

12.19 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to other organisation.

12.20 If such a request is made then the DPO must be consulted.

13 Data security

13.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

13.2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

13.3 Security procedures include:

13.3.1 **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the reception who will then inform the Head Teacher

13.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

13.3.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

13.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13.3.5 **USB and Hardware Devices.** The trust discourages the use of unencrypted USB and hardware devices. Systems are in place to prompt staff to encrypt these devices once they are plugged into a computer. Staff must encrypt their devices if they chose to use them.

13.3.6 **Working away from the school premises – paper documents.** Paper documents containing personal data should not be removed from the academy premises unless agreed by the Head Teacher and/or the Data Protection Officer. If documents are taken off site they must be concealed in a lockable bag and details must be documented, with a signed in/out procedure held in the main office.

13.3.7 **Working away from the school premises – electronic working.** Staff must work from a laptop that is encrypted when offsite. Equipment must be kept secured and not in a car.

13.3.8 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers. All printers which are not based in the main office should require a unique staff password before printing.

13.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14. Data Protection Impact Assessments

14.1 Take 1 takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

14.3 Take 1 will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

14.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

15. Disclosure and sharing of personal information

15.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, [and / or Education and Skills Funding Agency “ESFA”], Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

15.2 Take 1 will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

15.3 In some circumstances we will not share safeguarding information. Please refer to our Safeguarding and Child Protection Policy.

15.4 Further detail is provided in our Schedule of Processing Activities.

16. Data Processors

16.1 We contract with various organisations who provide services to the Take 1, including:

16.2 Payroll providers, information management service providers, IT and other data management contractors. The services delivered by these companies are integral to the work of the Take 1, including educational delivery in schools; record keeping including safeguarding records; analysis of data returns, and school improvement.

16.3 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

16.4 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Take1. Take 1 will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.5 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

17. Images and Videos

17.1 Parents and others attending Take 1 events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. Take 1 does not prohibit this as a matter of policy.

17.2 Take 1 does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of Take 1 to prevent.

17.3 Take 1 asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

17.4 As a community organisation and school we want to celebrate the achievements of our pupils and service users and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

17.5 Whenever a pupil begins their attendance at the Take 1 they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

18. CCTV

18.1 We operate a CCTV systems. Please refer to our CCTV Policy.

19. Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

ANNEX DEFINITIONS

Term	Definition
Data	Is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means 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
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by [School/Trust/Academy] such as staff and those who volunteer in any capacity including Governors [and/or Trustees / Members/ parent helpers]

Privacy Notice for Parents/Carers, Guardians and Pupils

This privacy notice advises parents, carers, guardians and pupils of the school's data protection responsibilities on the collection and processing of pupil's personal information.

You are being provided with this notice because either you can exercise your child's data protection rights on their behalf or for older children (usually when they reach the age of 13) they may be considered mature enough to exercise their own data protection rights.

This notice provides details about:

- The personal information we collect on pupils
- How we collect that personal information
- What we do with the personal information
- Your rights in relation to any personal information held and processed by the school

Take 1 is the overall 'Data Controller' of the personal data you provide to us. This means that they decide the purpose for which and the manner in which any personal data relating to pupils and their families is to be processed.

The Data Protection Officer for Take 1 is Naomi Fearon. Her role is to oversee and monitor the school's Data Protection procedures and to ensure they are compliant with GDPR.

Naomi can be contacted by telephone 0115 9708982 or by e-mail at

naomi@take1studios.co.uk

What is personal information and what does processing mean?

Personal information is any information that relates to your child that can be used directly or indirectly to identify them.

This includes information such as their name, date of birth and address as well as information relating to their exam results, medical details and behaviour records. This may also include sensitive personal information such as their religion or ethnic group, photos and video recordings.

Information that we hold in relation to you is known as your "personal data". This is information that we obtain from you directly and data about you that we obtain from other people and organisations. We might also need to continue to hold your personal data for a period after your child has left the school. Anything that we do with your personal data is known as "processing".

The lawful basis on which we use this information

Schools are required to hold data about all of their pupils. This is necessary so that we can meet our statutory obligations with the Local Authority, Department for Education and other key stakeholders.

We consider that we are acting in the public interest when providing education. Specifically, we have a public interest in:

- Providing an education

- Fulfilling our safeguarding obligations and investigating complaints that may be directly connected with or may require access to your personal data when investigating complaints by others
- Promoting the interests of the school and organisation
- Managing the school and organisation efficiently

Sometimes we may also use your personal information where the pupil or the parent/carer have given us permission to use it in a certain way or if we need to protect the pupils' interests (or someone else's interest).

Where we have permission to use the data, the pupil or the parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

What sort of data is collected?

The categories of pupil information that the school collects, holds and shares includes:

- Personal information, e.g. name, gender, date of birth, address
- Characteristics, e.g. ethnicity, language, nationality, country of birth, entitlement to free school meals
- Attendance information, e.g. the number of absences and the reasons for them
- Assessment information, e.g. national curriculum assessments results and on-going teacher assessments
- Relevant medical information
- Special Educational Needs and Disability (SEND) information (where appropriate)
- Behavioural information e.g. exclusions
- Accident/Incident information, e.g. where First Aid has been administered
- Equality information, e.g. incidents of racism, bullying
- Where the pupils go after they leave the school

Why do we collect and use this information?

- 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 to data sharing

Who we share pupil information with

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

We share pupils' data with the DfE on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to pass information about our pupils to the Department for Education (DfE) under regulation 4 of The Education (Information About Individual Pupils) (England) Regulations 2013.

We routinely share pupil information with:

- Schools that the pupil's attend after leaving us
- Our Local Authority
- The Department for Education (DfE)
- School Nurse
- A Third-Party IT services provider, named as CPOMS, for the purposes of securely holding and protecting your data.
- Alternative Providers of education, linked through the Local Authority
- GL Assessment

Youth Support Services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our Local Authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- • youth support services
- • careers advisers

A parent or guardian can request that only their child's name, address and date of birth is passed to their Local Authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our Local Authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- • post-16 education and training providers
- • youth support services
- • careers advisers

For more information about services for young people, please visit our Local Authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the DfE and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, Local Authorities and awarding bodies.

We are required by law, to provide information about our pupils 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 Pupils) (England) Regulations 2013.

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 pupils 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 pupils 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 Serena Sisson as detailed on the first page who will send you our Data subject's rights application form.

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 request 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/>

Contact

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

Naomi Fearon can be contacted by telephone 0115 9708982 or by e-mail at

naomi@take1studios.co.uk