Privacy Notice – Pupils

Date: May 2024
Review Date: May 2025
Version: 2
Document owner: Danielle Eadie

Vantage Academy Trust | Newport Road | Bolton | BL3 2DT

T: 01204 565 001 | E: questions@vantageacademies.co.uk

Introduction

The Vantage Academy Trust must collect and process the personal data of pupils and their families in order to fulfil our duties as an education provider. Under the UK General Data Protection Regulation (UK-GDPR), we must clearly inform individuals about the personal data we collect about them, why we have it and how we use it; this information is outlined in the following privacy notice.

Data Controller

The Vantage Academy Trust is the 'Data Controller' for the personal information that we process. This means that we are responsible for how it is processed and make decisions on how it is used.

Data Protection Officer

The trust has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation, namely the UK-GDPR and the Data Protection Act. Our DPO provides support to the trust and its schools and acts as the first point of contact for any questions or queries regarding data protection.

Our DPO is Miss Danielle Eadie from RADCaT Ltd who can be contacted via our respective school offices or directly using the following details:

T: 01942 590 785 | E: Danielle.eadie@radcat.co.uk

What information we process about pupils and their families?

The trust routinely collect the following types of information about pupils and their families upon admission and throughout their educational journey with us:

- Personal identifiers such as names, dates of birth, ID numbers including copy identification.
- Contact details including pupils, parents and emergency contacts.
- Characteristics: ethnicity, religion, pupil premium and free school meal eligibility.
- Allergies and dietary requirements.
- Accident and injury information.
- Special Educational Needs (SEN) and medical requirements.
- Safeguarding information and concerns.

- Attendance and absence information.
- Assessment and attainment information including pupil progress and reports.
- Behavioural information including details of any exclusions.
- Images taken as part of the curriculum and educational activities.
- Images recorded on CCTV around the school site (where applicable).
- Usage data relating to the internet and digital systems.

Please note that pupil usage of the internet and digital systems will be monitored by the trust to meet our requirements under Keeping Children Safe in Education (2023).

Where we get this information?

Most of the personal data that we collect is sourced directly from pupils and their families upon admission to one of our schools. Where applicable, the trust may also receive records from any previous schools or the local authority if it is relevant to their education with us.

As pupils progress through their educational journey with us, information is collated by the trust and our staff. Examples include logs of attendance, recording assessment information and updating SEN records when a development occurs.

Why we need the information?

Information about pupils and their families is used to meet the following purposes:

- To support pupil learning.
- To monitor and report on pupil progress.
- To enable the provision of services such as classroom resources.
- To safeguard pupils, their families and members of the community.
- To ensure the safety and security of our sites and the individuals we are responsible for.
- To provide pastoral support to pupils and their families.
- To meet the statutory duties placed upon us by the government and local authority.
- To promote our schools and provide and insight into school life within the trust.
- To ensure compliance and monitor the performance of the trust and its schools.

Is the processing of personal data optional?

Most of the information that we collect about pupils and their families to meet the purposes outlined above is mandatory to meet our legal and operational duties. The trust will inform parents at the point of collection whether or not processing is optional.

The following sections outline the lawful bases which we rely upon to process both mandatory and optional data.

The lawful basis for processing personal data

The trust must meet one of the lawful bases provided in Article 6 of the UK-GDPR to process personal data. When processing the personal data of pupils and their families, we routinely rely upon the following:

Legal obligations

The trust must process personal data to meet its **legal obligations**. For instance, when providing an education under the Academies Act, maintaining a safe environment for pupils under Health & Safety Law and submitting pupil data to the Local Authority and the Department for Education (DfE) to meet our statutory reporting duties.

Public task

The trust processes personal data for the performance of a **task in the interest of the public** for instance when providing health & social care, monitoring safeguarding concerns and supporting pupils with special educational needs.

Contractual obligations

The trust subscribe to online learning resources to help support pupils with their education. To provide access to such resources, we must process a small amount of pupil data usually to create a profile to access the activities and learning materials. In such instances, we are processing personal data to meet the terms of service we have with providers of classroom programs; we have a **contractual obligation**.

Consent

Where the processing of personal data is optional, the trust will seek consent. For instance, the trust seek consent for the use of pupil images to celebrate achievements and give the wider community an insight into school life.

Vital Interests

Less commonly, the trust may be required to share pupil, parent and emergency contact information with the emergency services if an incident or accident occurs. In such cases, we are processing personal data in the act of saving or protecting someone's life; their vital interests.

Special Category Data

Special Category Data is information about someone that is much more sensitive in nature and therefore data protection legislation requires us to provide additional safeguards to ensure it is safe, secure and processed lawfully. Examples of special category data include health information, ethnicity and religion.

When processing special category data, the trust must meet an additional lawful basis this time from Article 9 of the UK-GDPR. For the routine processing of special category data about pupils and their families, we rely upon the following:

- The **explicit (written) consent** of the parent or guardian for instance when sharing pupil health information with a third-party agency when additional support is required.

- **Substantial public interest** when processing data to meet our statutory and legal requirements for example when:
    - Sharing a pupil's gender, religion and ethnicity with the DfE as part of the school census for the purposes of equal opportunities monitoring.
    - Making a safeguarding referral to social services or the police to protect our pupils and their families in situations where consent is not appropriate.
    - Data is processed for the purposes of crime prevention and detection.

Less commonly, the trust must rely on the following conditions to process the special category data of pupils and their families:

- **Legal claims & judicial acts:** personal data is processed when supporting or defending a legal claim.
- **Vital interests:** where the trust may share details of any known medical conditions or allergies with emergency services in the act of saving or protecting someone's life.

Consent

Although pupil personal data belongs to them and not their parent or guardian, it is accepted that any consent for the processing of pupil personal data is sought from the parent or guardian. This is because children at a primary school age tend to be too young to understand data protection and their rights.

Where consent is the lawful basis for processing, parents can withdraw their consent or change their preferences at any time by contacting their respective school office.

Legislations & Guidance

When determining our lawful bases for the mandatory processing of pupil data, the trust are supported by the following legislation and statutory guidance:

- The Academies Act (2010)
- Education Act (1996)
- The Education (Information About Individual Pupils) (England) Regulations (2013)
- Education (Independent Schools Standards) Regulations (2014)
- Schools Admission Code (2021)
- Equality Act (2010) & Guidance for Schools (2014)
- Safeguarding Act (2006)
- Keeping Children Safe in Education (2023)
- Working Together to Safeguard Children (2018)
- Health & Safety at Work Act (1974)

Security, Storage & Retention of Data

To comply with the UK-GDPR, the trust only keep personal data for as long as necessary to meet our legal and operational duties.

The trust 'Records Management Policy & Retention Schedule' outlines how long pupil records are kept and how we determine and manage these periods. As a rule of thumb, pupil educational records are

kept by trust primary schools until the childs 18th birthday, whilst safeguarding and SEN records are kept until the pupil reaches 25.

Personal data about pupils and their families is stored securely on trust sites. Records kept in electronic format are stored securely on carefully selected databases and systems that are fully encrypted with password protection and two factor authentication utilised where available. Physical records are kept in locked cabinets within locked offices and archive rooms; key access is strictly limited depending upon role.

Trust staff and those third parties accessing key pupil records are subject to DBS checks and strict confidentiality agreements.

Who we share pupil information with?

The trust routinely share pupil and parent information with the following parties to meet our legal and statutory duties as an education provider:

- Local Authority
- Department for Education
- Pupil's next school or educational setting
- Auditors (Ofsted etc)

Further information can be found at **Appendix A** on statutory data sharing including the collections made by the Department for Education.

To support our operational activities, information about pupils is routinely shared with the following parties:

- Our staff and governors to allow them to perform their duties.
- Providers of educational resources such as classroom programs, software and apps to compliment educational development.
- Providers of software programs that allow us to effectively manage pupil information and their education with us.
- Providers of support services such as ICT & Catering to ensure they can effectively fulfil their commitments to the trust.

Please note that the support services and software programs used may differ from school to school, please contact us if you would like an up-to-date list from your respective school.

In certain circumstances, the trust may share information about pupils and sometimes their families with the following parties:

- Third party support agencies relating to health if there is a special educational need.
- Social services and / or the police if there is a significant safeguarding concern.
- Emergency services if an accident or injury has occurred.

Less commonly and only in certain circumstances, the trust may be required to share data about pupils and their families with the following parties:

- Professional advisors to the trust in situations where we may need to seek further support or legal advice for instance with our solicitors if a claim is made against the school.
- Police and other enforcement authorities in the act of preventing or detecting criminal acts.

- Courts in situations where the trust must support or defend a claim.
- Insurance providers if the trust require financial support as a result of a claim.

Keeping data sharing secure and compliant

When sharing information with third parties, the trust adopt a minimal approach to ensure only the necessary information is shared. Similarly, no data is shared with third parties unless the trust is satisfied that the recipient is authorised to receive the information and a secure method of transfer is available.

Third party providers of services to the trust that must access personal information are subject to compliance checks and strict data sharing agreements to ensure they meet the trusts high standards of security and comply with data protection legislation.

International data transfers

We do not routinely transfer personal data outside of the United Kingdom, however some providers of key services to the trust may store a very limited amount of personal data on servers outside of the UK usually within the European Economic Area (EEA) who have the same strict privacy laws as ourselves in the UK. Where this is applicable, we ensure that such providers meet our high standards of security and comply with the relevant data protection law.

Requesting access to your personal data and your rights

Individuals have a number of rights in relation to their own personal data; parents can also exercise theses rights on behalf of their child in trust primary schools: In certain circumstances, parents have the right to:

- Ask us about the information we hold about you and your child and request copies of the information by making a 'subject access request'.
- Ask us to rectify any information that you feel is inaccurate or incomplete.
- Ask us to erase the personal information about you and your child in certain circumstances.
- Ask us to restrict or object to the processing of yours or your childs personal information if you do not feel we have legitimate grounds to do so.
- Object to the processing of yours or your childs personal data in situations where processing is optional; we have asked your permission.
- Not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.

If you would like to find out further information or make a request relating to your rights, please contact the office of your respective school in the first instance.

The school office along with the trust Data Protection Officer (DPO) will support you with your request; a response will be provided within one calendar month. The school has a legal right to extend this period by a further two months for any requests deemed excessive, we will however inform you of our intentions to extend the response time within one calendar month.

Complaints

If you have any concerns at all about how we process your personal data, please contact us in the first instance so that we can help resolve any issues.

You can also complain to the Information Commissioners Office (ICO) if you are unhappy with how we have used your data:

Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline: 0303 123 1113

Website: https://www.ico.org.uk

Appendix A – Why we must share pupil data?

Data shared between educational settings.

When a pupil transitions between educational settings such as from primary to secondary school, their pupil record moves with them; this is a legal obligation placed on the school to allow each setting to adequately provide an education and support to pupils. Any transfers completed between educational settings are carried out using secure file transfer systems including the DfE's school to school system (S2S) and the Child Protection Online Monitoring and Safeguarding system (CPOMs).

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

The National Pupil Database (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 Students to the DfE as part of statutory data collections; the school census is an example of when we share data. 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 DfE 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 DfE 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. All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

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 Student 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