Brook Learning Trust
Data Protection Policy and Privacy Notice

At Brook Learning Trust we bring together our unique academies in our belief in the power of education to change lives and communities. It is our steadfast purpose to challenge and defy the barriers that constrain the educational progress of any child. We set high aims for aspiration and secure collective responsibility for all our children's achievements. Our work is underpinned by the values of Integrity, Respect, Courage, Optimism, Excellence and Accountability.

Aims & Objectives of this Policy
The aim of this policy is to provide a model set of guidelines to enable staff, parents and pupils to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data
- How CCTV is used, processed, stored, and deleted/destroyed.

The objective of the policy is to ensure that Trust Academies act within the requirements of the General Data Protection Regulation 2018 (GDPR) and The Data Protection Act 2018 when collecting, using, sharing or disposing of personal data. This policy also outlines the process for supporting requests from individuals who wish to exercise their rights in relation to personal data.

Data Protection – The guiding principles of using personal data

- Information relating to people which is held in a form that allows them to be identified is known as personal data
- The use of personal data will be undertaken both fairly (in accordance with the rights of individuals) and lawfully (in accordance with the GDPR 2018, The Data Protection Act 2018, and other associated legislation
- The purpose(s) for collecting, using and sharing data will be declared in a way that lets individuals understand how and why their personal data is being used and also who it is being shared with
- The collection, use and sharing of personal data will be limited to only what is necessary to achieve the purpose(s) declared, where there is a legal obligation to do so, where consent has been sought, or some other lawful condition for processing has been met
- The accuracy of personal data will be proactively maintained for the duration of time it is being used
- Personal data will be held only for as long as it necessary or where there is a legal requirement to retain it
- There will be organisational and technical measures put in place to ensure that where possible, personal data is not lost, misused, shared inappropriately or destroyed (unlawful processing).

The Rights of Individuals

- Everyone has the right to be informed about how their personal data is being used. We adhere to this right by publishing Privacy Notices for pupils and parents and for staff which can be found at Appendices 1 and 2
- Under the GDPR 2018, the Data Protection Act 2018, and other associated legislation, individuals have the right to access their personal data. This may include parents, pupils, members of staff, or other people. For pupils, it may be necessary to consider if they are of an age to understand the information they request. Parents (as defined in the Education Act 1996) may also request access to their child's personal data. The process for accessing information about yourself "Subject Access" can be found here http://www.brooklearningtrust.org.uk/SAR

- Anyone has the right to rectification, where inaccurate information is being held or used, but this must pertain to matters of fact, not of opinion. If the information we hold about you is inaccurate you can request that it is amended, or that the use of this information is restricted (temporarily) by emailing dpo@brooklearningtrust.org.uk. We may ask you to provide supplementary documents or evidence to help determine the accuracy of information.
- In certain circumstances individuals may be able to exercise the right to be forgotten (erasure). This is not an absolute right and there are not many instances where information being processed by an academy can be considered when an individual wants to exercise this right
- Individuals have the right to object to processing. This may occur when someone decides to withdraw their consent from the use of their personal data for a specific purpose, For example, a parent may wish to withdraw consent for their child's image to be used in publicity materials. A request of this nature must be made in writing to dpo@brooklearningtrust.org.uk.

Keeping Information Safe

- Confidentiality should be respected. Personal data should always be kept securely and protected by passwords if they are electronic. Access to personal data should be confined to those authorised to see them. The law also provides that personal data should not be kept longer than is required
- Third party data (information about someone other than the requesting individual) should in general only be provided with the permission of that party, or where a formal contract, or agreement is in place to manage the transfer of information
- Information should only be shared outside of the academy using appropriate secure technologies where these are available and care should also be taken when transferring or transporting paper records which contain personal data
- A named person will have overall responsibility for personal data within each academy. In most cases this will be the Principal.

Staff in academies will be trained on the appropriate use of personal data. This training will take place as part of induction and then at least annually.

Failure by staff to comply with this policy puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the Trust and may in some circumstances amount to a criminal offence by the individual. Any failure to comply with this policy may lead to disciplinary action under the Trust's procedures.

The Information Commissioner's Office may also take action against individuals who willingly misuse or unlawfully process personal data that they are responsible for.

Reporting Data Breaches

All staff will be made aware of the 'breach reporting' process to ensure that any loss, misuse or inappropriate sharing of data is reported quickly and effectively to allow action to be taken within the mandatory timescales for reporting.

All data security breaches, including 'near misses', must be reported immediately to enable the Data Protection Officer and GDPR Leads to assess the breach, advise on the necessary steps that need to be taken, to contain any resultant damage and inform individuals who may be affected. A central record of all breaches will be retained and any serious breaches will be reported to the Information Commissioner's Office within the 72 hour timeframe set out.

Guidance for Processing, Storing, Archiving and Deleting Personal Data:

- The "processing" of personal data includes its collection, storage, use, sharing, retention and disposal.
- Every individual within the Trust has a responsibility to ensure personal data is processed in a lawful manner
- Personal data and school records about pupils should be treated as confidential information and protected accordingly

- Once collected, information should be stored in appropriate files and systems that are relevant to the purposes the information is required for
- Information can be shared appropriately within the professional working of the academy to support the delivery of teaching and learning and the provision of safeguarding duties. The law also permits such information to be shared with other educational establishments when pupils change schools, central and local government agencies performing statutory duties and other organisations with whom the Trust has an approved contract or agreement in place
- Information should only be kept for as long as is necessary
- The Trust has adopted the guidance developed by IRMS in its Information Management Toolkit for schools, to inform the retention of documents containing personal information. A copy of this guidance is available to view online : https://irms.org.uk/page/SchoolsToolkit
- School and examination records for a child should be kept for seven years after the child leaves the establishment, or until the child reaches twenty-five years of age (whichever is greater)
- Data on staff are sensitive information and should also be treated as confidential records. They are shared, where appropriate, at the discretion of the Principal and with the knowledge, and where necessary, the agreement, of the staff member/s concerned, unless there is a legal requirement to do so
- Employment records form part of a staff member's permanent record. Because there are specific legislative issues connected with these (salary and pension details etc) employment records should be retained for the duration of a staff member's employment and for a further seven years after the cessation of employment
- Interview records, CVs and application forms for unsuccessful applicants will be kept for six months

All formal complaints made to the CEO, Principal, Trust Board or Academy Council will be kept for at least seven years in confidential files, together with any documents relating to the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection recommendations and to legal professional privilege in the event of a court case.

CCTV data

CCTV at Trust academy sites (The Hayesbrook School and The High Weald Academy) is owned and managed by the academy. It is used to ensure the security of the site and those who work there by monitoring areas of the academies that cannot be continually and/or directly supervised by members of staff. CCTV at The Ebbsfleet Academy is partly owned and managed by Pinnacle, the site management contractor; however, some of these cameras may be operated at the academy by Brook Learning Trust. Additional cameras at The Ebbsfleet Academy are owned and managed by the academy to ensure coverage of vulnerable areas of academy activity.

The use of CCTV will:

- Act as a deterrent to crime and anti-social behaviour, both during the day and outside normal academy hours
- Support the academies' behaviour management policies
- Monitor the behaviour of visitors to the site
- Reduce incidents of vandalism, aggression and poor behaviour and will make it easier to identify those responsible should such incidents occur.

The following is to establish a framework that meets both the needs of each academy and guarantees that the rights of individuals (whether they are staff, students, parents or members of the public) are not compromised. It will do this by:

- Operating in a way that meets the legal requirements of the GDPR 2018 and Data Protection Act 2018 and other relevant legislation
- Establishing clear operating protocols and lines of accountability.

CCTV Procedures

- Overall responsibility for the management and use of CCTV rests with the Principal of each academy and will be monitored by the Academy Council and the Trust Executive

- Day to day monitoring of the CCTV to ensure that it is working effectively will be the responsibility of the member/s of staff at each site to whom this responsibility has been allocated. A daily log will be kept of all defects and actions taken
- Signs will be clearly displayed in obvious locations at each relevant site informing people that CCTV surveillance is in operation
- Cameras will be located to take into account areas where privacy is expected
- Images will be stored on each hard drive for a minimum period of 14 days and where possible, for a maximum of 49 days. All images will be overwritten automatically at the end of this period.

Access to CCTV data

- Access to stored data will be limited to those members of staff at each academy tasked with checking the footage. Access may only be granted to other members of staff by the Principal or the CEO of the Trust
- A log will be kept of all incidents where images are viewed, detailing who accessed them and when and why they were accessed. Staff who view images are not permitted to copy or remove these images without the permission of the Head of School, Principal or CEO
- In some cases images/video may have to be downloaded to prevent them from being erased, for example for use as evidence in an investigation. Images/video may only be downloaded and stored by members of staff with the permission of the Head of School, Principal or the CEO of the Trust. They must be kept securely and destroyed once the need for them to be stored has passed
- External access to stored images will only be granted to authorised persons where there is a clear legal obligation, such as a court order or where the request comes from the police as part of an investigation into criminal activity
- Any requests for subject access should be referred to the Principal, the Data Protection Officer, or the CEO of the Trust both for authorisation and for agreement about the position of images that relate to third parties
- A disclosure log will be kept, detailing any individual or organisation that has been supplied with stored images and the reason why they were requested.

Reference: CCTV Code of Practice published by the Information Commissioner's Office, found at: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Biometric information

Biometric data is information linked to a reading or measurement of a person's biological features or characteristics: most commonly fingerprints or palm prints, iris or retina scans and other facial recognition technology, including DNA.

Brook Learning Trust's schools use biometric data in the form of fingerprints to operate cashless purchasing systems to allow staff/pupils to buy food and provide a record of meals purchased.

Sections 26 to 28 of The Protection of Freedoms Act 2012 include provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. The Act states that:

- Written consent is required from at least one parent for all pupils under the age of 18 where biometric data personal information is used in an automated recognition system
- Schools do not need to have written consent from the pupil, however they do need to respect pupils' wishes should they refuse to participate. A pupil's objection will always override parental consent in this regard and the objection of one parent can override the consent of another. Consent may also be withdrawn at any stage
- Reasonable alternative arrangements must be provided for pupils or staff who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to the pupil's own refusal or the staff member's refusal to participate
- Alternative arrangements ensure that pupils and staff do not suffer any disadvantage or difficulty in accessing services as a result of them not participating.

All parents are asked to complete a biometric data consent form for their child for the purpose of purchasing food and providing a record of meals purchased. All staff are offered the opportunity to provide their biometric data (fingerprint) for the same purpose.

The consent form will clearly state which external bodies this data will be shared with in order to provide our catering services. The data that is held will not be used by any other organisation for any other purpose, other than those stated in the consent form. It is the responsibility of the school and external body to ensure that the information is stored securely.

Once a pupil or member of staff stops using the biometric recognition system, their biometric information will be securely deleted by the school and/or the external body in accordance with the Information Commissioner's Office Guidance.

Further information and guidance can be found in the Department for Education's 'Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff':
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf

Recording of Meetings and Lessons (onsite or virtual)

On occasion, meetings or lessons may be recorded by the Trust or academy in order to enable minute takers to fulfil their task, enable meeting participants (or non-attendees) to access a recording of a meeting, enable students to access a recorded lesson or to support safeguarding of students. This may include the recording of audio or video of the attendees.

Participants will not be required to give consent for these recordings, however they will be informed that recording is taking place and the purpose of the recording. Recordings will be held securely within the academy or central Trust and once the need for the recording has been completed it will be deleted.

Participants may not record meetings/lessons, or any part of the meeting/lesson without receiving the explicit consent of all those participating and stating the purpose of the recording.

Accessing Personal Data: Guidance

- A child can request access to his/her own data. The request is not charged and does not have to be in writing. The staff member with overall responsibility for personal data within the academy will judge whether the request is in the child's best interests and whether the child will understand the information provided. He/she may also wish to consider whether the request has been made under coercion
- A parent can request access to or a copy of his/her child's school records and other information held about their child. The request must be made verbally or in writing. There is no charge for such requests on behalf of the child, but there may be a charge for photocopying records: this is detailed in guidance available from the Information Commissioner. Staff should check, if a request for information is made by a parent, that no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force
- Parents should note that all rights under GDPR and Data Protection Act to do with information about their child rest with the child as soon as they are old enough to understand these rights.
- Separately from the Data Protection Act, The Education (Pupil Information) (England) Regulations 2005 provides a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. Parents who wish to exercise this right must apply to the academy in writing
- All requests for personal data (Subject Access Requests) will be dealt with as soon as possible, or within a 30 day timescale. Unless the request is deemed to be complex or multiple requests have been received from an individual and in these cases an additional two months can be used for dealing with requests
- Educational records: (unlike other personal data) access must be provided within fifteen school

days and, if copies are requested, these must be supplied within fifteen school days of receipt of any payment due

- A member of BLT staff can request access to their own records. The member of staff has the right to see his/her own records and to ask for copies of the records.
- All requests will be acknowledged in writing on receipt and access to records will be arranged as soon as possible. If awaiting third party consents, the Trust/academy will arrange access to those documents already available, and notify the individual that other documents may be made available later
- In all cases, should third party information (i.e. information about another individual) be included in the information, permission will be sought to show this information to the applicant, with the exception of information provided by another member of Trust staff or an agency representative who is exempt from a requirement for third party consents. If third party permission is not obtained, the person with overall responsibility should consider whether the information can still be released
- Personal data only relates to information held in records where individuals are identifiable. For example, a document discussing more general concerns, but not identifying a specific individual, may not be defined as personal data. If it is unclear whether a record contains personal data, advise should be sought from the Data Protection Officer
- Anyone who requests to see their personal data has the right to question the accuracy of matters of fact recorded in the data, and to ask to have inaccurate information deleted or changed. They may also question opinions and their comments will be recorded, but opinions do not need to be deleted or changed as a part of this process
- The Trust/academy will document all requests for personal information, including details of who dealt with the request, what information was provided and when, and any outcomes (letter requesting changes etc.). This will enable staff to deal with a complaint if one is made in relation to the request.

Fair Processing of Personal Data: Data Which May be Shared

Trusts, academies, local education authorities and the Department for Education (DfE) all hold information on pupils in order to undertake their duties as public authorities and in doing so have to follow GDPR and Data Protection Act 2018. This means, amongst other things that the data held about pupils must only be used for specific purposes allowed by law. The Trust has a Privacy Notice which explains how personal data are used and with whom they will be shared. This Privacy Notice can be found at Appendix 1.

The Trust and the relevant education authorities which oversee its academies use information about pupils to carry out specific functions for which they are responsible, such as the assessment of any special educational needs the pupil may have. They also uses this information to derive statistics to inform decisions on (for example) the funding of schools, and to assess the performance of academies and set targets for them. The statistics are used in such a way that individual pupils cannot be identified from them.

Information on how to access personal data held by other organisations is given below.

Pupils, as data subjects, have certain rights under the Data Protection Act, including a general right of access to personal data held on them, with parents exercising this right on their behalf if they are too young to do so themselves. If your child wishes to access his/her personal data, or you wish to do so on his/her behalf, please email dpo@brooklearningtrust.org.uk, or contact the Principal of your child's school in writing.

POLICY REVIEW AND RATIFICATION

Policy reviewed by the Trust Executive every two years and ratified by BLT Board in May

This review by BLT Executive and IT Managers	May 2020
Summary of amendments to this iteration	Additional detail added regarding reporting data breaches. Additional clarity given regarding the processing, storing, archiving and deleting of personal data. Inclusion of section on the recording of lessons and virtual meetings.
Ratified by the Trust Board	May 2020
Next Review due	May 2022
Next Ratification	May 2022

Bibliography
(Urls last accessed April 2020)

Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Information Commissioner's Office, Publication of Examination Results by Schools:
https://ico.org.uk/for-the-public/schools/exam-results

Information Commissioner's Office, Accessing Pupils' Information:
https://ico.org.uk/for-the-public/schools/pupils-info

Disclosure & Barring Service:
Code of practice for registered persons and other recipients of disclosure information through the DBS checking service https://www.gov.uk/government/publications/dbs-code-of-practice

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972:
Retention requirements http://www.hse.gov.uk/foi/retention-schedule.htm

Sections 26 to 28 of The Protection of Freedoms Act 2012
http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/2/enacted

Brook Learning Trust

Example Privacy Notice for Pupils and Parents

Appendix 1 of the BLT Data Protection Policy

*****Each academy has an individual privacy notice for pupils and parents, which can be found on the policy page of their website.*****

Who processes your information?
Brook Learning Trust and its academies are the data controllers of the personal information you provide to us. This means the Trust and its academies are responsible for deciding how information you provide us with is used. We refer to your information as "personal data" and when we use your information in different ways, this is called "processing". The General Data Protection Regulation (GDPR) 2018 outlines how personal data should be protected and used appropriately by organisations.

In some cases, your personal data will be shared with other people, organisations or companies. This sharing will only occur after we have sought your permission (consent), unless the law requires us to do so. If we share your personal data outside of school, we ensure that the same data protection standards are upheld by other people involved in processing your personal data.

The categories of pupil information that we process include:

- Personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- Personal identifiers and contact information for parents and carers (such as names, addresses, telephone numbers, email addresses)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Safeguarding information (such as court orders and professional involvement)
- Images (such as photographs and CCTV images)
- Special educational needs
- Medical and administration (such as doctors information, student health, allergies, medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment, attainment and progress information
- Examination information (including entries and results)
- Behavioural information (such as exclusions and any relevant intervention or alternative provision put in place)
- Assessment and examination information
- Welfare information
- Post 16 learning information.

Why do we collect and use your information?
Brook Learning Trust and its academies hold the right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, Local Authority and/or the Department for Education (DfE). We collect and use personal data

in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- To keep children safe (food allergies, or emergency contact details)
- To meet the statutory duties placed upon us for DfE data collections.

Which data are collected?

- Personal information – eg names, pupil numbers and addresses
- Characteristics – eg ethnicity, language, nationality, country of birth & free school meal eligibility
- Attendance information – eg number of absences and absence reasons
- Assessment information – eg national curriculum assessment results
- Relevant medical information
- Information relating to SEND
- Behavioural information – eg behaviour incidents and temporary exclusions
- Photographs – Your child's photograph will be captured by our chosen external school photography company, Tempest (for The High Weald Academy and The Hayesbrook School) and Van Cols (for The Ebbsfleet Academy) and will be made available for you to purchase. These images will be used to aid our records management, safeguarding and attendance procedures. Historical images of students will be retained after they have left the academy
- Assessment and examination information
- Welfare and other pastoral support information
- Biometric information – eg digital finger prints to support our cashless catering and payment systems.

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

Sometimes, we may also use your personal information where:

- You or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest).

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

The categories of parent information that the Trust/academy collects, holds and shares includes the following:

- Contact information, including addresses, phone numbers and email addresses of parents and/or any other emergency contacts
- Financial information where appropriate, e.g. to check eligibility for Free School Meals
- Information pertaining to home life where appropriate, e.g. where a pupil is identified as

having a mental health issue or there are safeguarding concerns.

How long is your data stored for?
Personal data relating to pupils at a Brook Learning Trust academy and their families are stored in line with the Trust's Data Protection Policy.

In accordance with GDPR, the Trust and its academies do not store personal data indefinitely; data are only stored for as long as is necessary to complete the task for which they were originally collected.

Will my information be shared?
The Trust and its academies are required to 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 share information about our pupils with the DfE under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Brook Learning Trust and its academies are required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing 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 any data shared from the NDP is maintained.

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

Why we regularly share pupil information
The Trust and its academies do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. The school routinely shares pupils' information with:

- Your family and representatives
- The DfE
- The Local Authority (Kent County Council)
- The local NHS Trusts
- Pupils' destinations upon leaving the academy
- Educators and examining bodies
- Providers of our education welfare services
- Providers of our education psychology services
- Providers of our student counsellor services
- Our external auditors
- Survey and research organisations
- Health and Social welfare organisations
- Professional advisers and consultants
- Police and PCSO services
- External sports coaches
- CAMHS (Child and Adolescent Mental Health Service)
- Local forums with schools and relevant Local Authority representatives which support in-year fair access processes and support managed moves between schools
- Local multi-agency forums which provide SEND advice, support and guidance (such as Local

Inclusion Forum Team (LIFT))
- Other academies within our Trust, to enable the moderation of pupil assessment outcomes
- Our regulator, Ofsted
- Platforms such as Google Classrooms, Google Meet, Loom - for the purpose of virtual meetings and lessons
- Contracted providers of services (such as school photographers and catering providers) where consent has been given.

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.

The information shared is limited to the child's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach 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.

What are your rights?
Parents and pupils have the following rights in relation to the processing of their personal data.

You have the right to:
- Request access to the personal data that the Trust and its academies hold
- 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
- Request that your personal data is amended if it is inaccurate or incomplete
- Request that your personal data is erased where there is no compelling reason for its continued processing.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

Where can you find out more information?
For more information about the DfE'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 DfE has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/dfe-external-data-shares

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

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

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information held about them. To make a request for your personal information, or be given access to your child's educational record, contact our Data Protection Officer via dpo@brooklearningtrust.org.uk or by writing to Brook Learning Trust, The High Weald Academy, Angley Road, Cranbrook, Kent TN17 2PJ. Please address letters: For the attention of 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
- A right to seek redress, either through the ICO, or through the courts.

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly with 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: dpo@brooklearningtrust.org.uk.

Brook Learning Trust

Privacy Notice for Staff, Volunteers, Trustees, Members and Academy Councillors

Appendix 2 of the BLT Data Protection Policy

Who processes your information?
Brook Learning Trust is the data controller of the personal information you provide to us. This means the Trust is responsible for deciding how information you provide us with is used. We refer to your information as "personal data" and when we use your information in different ways, this is called "processing". The Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2018 (GDPR) outlines how personal data should be protected and used appropriately by organisations.

In some cases, your personal data may be shared with other people, organisations or agencies as necessary. This sharing will only occur if we have a legal obligation or duty to do so or after we have sought your permission (consent). If we share your personal data outside of the Trust, we ensure that the same data protection standards are upheld by other people involved in processing your personal data.

The categories of staff / governance information that we process include

- Personal identifiers and contacts (such as name, date of birth, employee number, national insurance number, contact details, address, next of kin and emergency contact numbers)
- Characteristics (such as ethnicity, gender, age)
- Recruitment and safeguarding information (such DBS check, copies of right to work documentation, references and other information included as part of the application process)
- Relevant medical information (such as doctor's details, medical conditions, allergies)
- Work absence information (such as number of absences and reasons)
- Qualifications and employment records, including work history, job titles, working hours, training records, professional memberships, outcomes of disciplinary and/or grievance procedures
- Payroll information (such as salary, pension and benefits information, bank details, position, start date)
- Governance details (such as role, start and end dates and governor ID)
- Photographs – Your photograph will be captured by the IT Network Manager or our chosen external school photography companies, Tempest and Van Cols, and may be made available for you to purchase. These images will be used to aid our records management and safeguarding procedures. Historical images of staff will be retained after they have left the academy
- CCTV images.

Why do we collect and use your information?
Brook Learning Trust holds personal data relating to employees, members of our Trust Board / Academy Councils and individuals who may visit or support the Trust in other ways. We may also receive information from previous employers, Local Authorities and/or the Department for Education (DfE). We may share personal data with other agencies as necessary under our legal obligations or otherwise in accordance with our duties as a Trust.

We will use your personal information for the following:

- The recruitment process and for carrying out pre-employment checks
- Safeguarding students
- Checking your identity and right to work in the United Kingdom
- Checking your qualifications
- To keep an audit trail of the checks we have made and our relationship with you in case of

employment claims
- To set up payroll and pension, and to reimburse expenses
- Communicating with you, including for marketing purposes
- Carrying out our role as your employer or potential employer.

We use workforce data to:

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

We use governance data to:

a) Meet the statutory duties placed upon us.

We collect and use personal data in order to meet our legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR;
- Education Act 1996.

All academy Trusts, under the Academies Financial Handbook have a legal duty to provide the governance information as detailed above.

Whilst the majority of the personal data you provide is mandatory, some is provided on a voluntary basis. You will be informed whether you are required to provide this data or if it is requested on a voluntary basis.

How long is your data stored for?

Your personal data will be held securely in line with the Trust's Data Protection Policy and IRMS records management toolkit guidance on retention (https://irms.org.uk/page/SchoolsToolkit).

In accordance with GDPR, the Trust does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which is was originally collected.

Who we share workforce information with?

The Trust will routinely share information with:

- The DfE
- The Education and Skills Funding Agency (ESFA)
- The Local Authority and its agencies
- HM Revenue and Customs
- Teacher Regulation Agency
- Companies House (for Trustees, Members and Company Secretary)
- The Trust's external auditors – MHA MacIntyre Hudson
- The Trust's internal auditors – William Giles
- The Trust's/Academy bankers – Lloyds Bank
- Teacher / Local Government Pension Services
- National Governance Association (for Academy Councillors, Trustees and Members)
- Data Protection services providers – Services4Schools and GDPRiS
- Providers of our IT infrastructure, e.g. Google and Microsoft
- Individual applications that support teaching and learning within our academies
- Providers of our visitor management app - All Things Code (staff at The Ebbsfleet Academy)
- The Trust's eLearning provider - TES Global.

From time to time, we may also need to share your information with other third parties including the following:

- Other Government agencies (where required)
- National Health Service (including the NHS Test and Trace service)
- The Trust's Occupational Health providers – Preventative Healthcare Company Ltd and

Maitland Medical Occupational Health
- The providers of therapy and support services (working with pupils in school)
- Disclosure and Barring Service
- The Police and law enforcement agencies
- The Courts, if ordered to do so
- The Trust's legal services provider – Browne Jacobson
- Staff Working Conditions and Wellbeing survey provider – Edurio
- Unions
- Joint Council for Qualifications
- Prevent teams in accordance with the Prevent Duty on schools
- Virtual meeting platforms, including WebEx, Google Classrooms, Google Meet, Loom - for the purpose of virtual meetings and lessons
- PFI contractors – Pinnacle (staff at The Ebbsfleet Academy)
- DfE Risk Protection provider (Top Marks Claims Management UK)
- Schools Advice Service – insurance services
- Vacancy Filler online recruitment platform.

Why we share workforce information
We are required to share information about our Trust employees with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Why we share governance information
All data is transferred securely and held by the DfE under a combination of software and hardware controls which meet the current government security policy framework.

We are required to share information about our Trustees and Academy Councillors with the DfE under the requirements set out in the Academies Financial Handbook.

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

The governance data we share with the DfE is entered manually on the GIAS system and held by the DfE under a combination of software and hardware controls which meet the current government security policy framework.

The Trustee/Academy Councillor data that we lawfully share with the DfE via GIAS:
- Will increase the transparency of governance arrangements
- Will enable schools and the department to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context
- Allows the department to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role.

How the Government uses your data
The workforce data that we lawfully share with the DfE through data collections:
- Informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- Links to school funding and expenditure
- Supports 'longer term' research and monitoring of educational policy.

Data collection requirements
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.

Sharing by the Department of Education
The DfE may share information about Trust 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 DfE 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 the 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.

To contact the Department of Education: https://www.gov.uk/contact-dfe

What are your rights?
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, contact our Data Protection Officer at dpo@brooklearningtrust.org.uk or by writing to Brook Learning Trust, The High Weald Academy, Angley Road, Cranbrook, Kent TN17 2PJ. Please address letters: **For the attention of 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
- A right to seek redress, either through the Information Commissioner's Office (ICO), or through the courts.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

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

Where can you find out more information?
For more information about the Department of Education's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

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

Requesting access to your personal data
Under data protection legislation, staff and volunteers have the right to request access to information held about them. To make a request for your personal information, contact our Data Protection

Officer at dpo@brooklearningtrust.org.uk or by writing to Brook Learning Trust, The High Weald Academy, Angley Road, Cranbrook, Kent TN17 2PJ. Please address letters: For the attention of the Data Protection Officer.