THE BENTLEY WOOD TRUST

DATA PROTECTION POLICY Inc Privacy Notices & Subject Access Request Procedures

GB Committee Responsible:	**Board of Directors**
Reviewed by:	Kieran Robinson/Paola Boyadjian/Marion Tam
Review Date:	June 2025
Ratified by Local Committee:	
Ratified by the Board:	10th July 2025
Next Review Date:	June 2027

Statement of Intent

The Bentley Wood Trust is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the UK GDPR.

The schools may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how each school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and The Bentley Wood Trust believes that it is good practice to keep clear practical polices, backed up by written procedures.

Contents

1. Introduction

The Bentley Wood Trust, comprising Bentley Wood High School and Aylward Primary School, collects and uses personal information about staff, students, parents and other individuals who come into contact with the schools. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that each school complies with its statutory obligations.

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Staff is defined by employees, governors, trustees and volunteers. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up and including dismissal depending on the seriousness of the breach.

2. Aims

Our Trust aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

3. Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, and other related legislation. It will apply to all personal data regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

4. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.
It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

5. Definitions

Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Categories of Personal Data –

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data.

Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

-

Processing – Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.
Processing can be automated or manual.

Data Subject – An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Data Controller – The organisation storing and controlling such information (i.e., the School) is referred to as the Data Controller.

Processing - Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing - Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA) - DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Data Breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Pseudonymised - The process by which personal data is processed in such a way that that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.
Criminal Records Information - This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

6. The Data Controller

Our schools process personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.
The Bentley Wood Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. Registration Reference: Z2768715.

7. Roles and Responsibilities

This policy applies to **all staff** employed by our schools, within the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

7.1 Governing Board

The governing board has overall responsibility for ensuring that each of our schools complies with all relevant data protection obligations. UK GDPR will be a regular agenda item for both schools.

7.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The DPO reports to the highest level of management in the Trust, which is the Board of Directors.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school/Trust data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
Full details of the DPO's responsibilities are set out in their job description.

The contact details for our Data Protection Officer (DPO) are as follows: -

Data Protection Officer: Judicium Consulting Limited Address:
5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Lead Contact: Craig Stilwell

7.3 Headteacher

The Headteacher of each school acts as the representative of the data controller on a day-to-day basis.

7.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

8. Data Protection Principles

The School are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR.

The principles the School must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The School only collect, process and share personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The School may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The School may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing in necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

Criminal Record Data

Where criminal records data is processed, a lawful condition for processing that data is also identified and documented.

Consent

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.In cases of processing special category data and explicit consent, the School will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The School will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data. [Please refer to the School's Data Retention Policy for further guidance].

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Retention Policy for further details about how the School retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to assure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

9. Sharing Personal Data

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our School shall be clearly defined within written notifications and details and basis for sharing that data given.

9.1 Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

9.2 Transfer of Data Outside the UK

The School may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules,

standard data protection clauses or compliance with an approved code of conduct.

Privacy statements for staff and students/parents can be found in Appendix 1.

10. Data Subject's Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.
The rights data subjects have in relation to how the School handle their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the School's processing activities;

(c) Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);

(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) Make a complaint to the supervisory authority, which is the Information Commissioner in England and Wales https://ico.org.uk/global/contact-us/; and

(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

11. Direct Marketing

The School are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

12. Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example, by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction [Please refer to the School's Information Security Policy for further details about our security processes]);
- Not remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;

- Not store personal information on local drives.

13. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

14. Biometric Recognition Systems (Bentley Wood High School only)

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, we will issue a PIN number to individuals who have not consented.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

15. CCTV

We use CCTV in various locations around each school's site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. For further detail see CCTV Policy.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Operations Manager (Bentley Wood) or School Business Manager (Aylward).

16. Photographs and Videos

As part of our schools' activities, we may take photographs and record images of individuals within our schools and on supervised authorised educational activities outside school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials and to improve educational provision.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within each school on notice boards, displays and in school magazines, brochures, newsletters, etc.
- Outside of each school by external agencies such as the school photographer, newspapers, campaigns

- Online on our schools' websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child except first name and year group, to ensure they cannot be identified.

17. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as Co-Pilot, ChatGPT and Google Bard. The Bentley Wood Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, The Bentley Wood Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in The Bentley Wood Trust Data Breach Policy.

18. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, staff handbook and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Please find below details of the School's Data Protection Officer: -
Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines. Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the School to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed [but would refer you to the School's Data Retention Policy in the first instance];

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach [and would refer you to the procedure set out in the School's Data Breach Policy];

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

19. Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the School conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data. In any event the School carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

20. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use and keys kept secure.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff, other than SLT/SLG must gain approval from SLT/SLG prior to doing this.
- Passwords that are complex are used to access each school's computers, laptops and other electronic devices:

Minimum of 9 characters
3 random words (no spaces) – not family/pet names or something easy to guess like onetwothree
Upper and lower case letters

.

Staff and students are required to change their password every 60 days.

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Only USB devices authorised by the school are able to connect to school devices, all others

are blocked.

- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT/Online Safety Policy including Acceptable Use Agreement).
- Each school has systems in place to protect themselves from cyber crimes including:
    - Registered with the police CyberAlarm
    - 2-factor authentication if accessing the school network when off-site
    - Regular updates and patches applied
    - No access to the schools' networks from 10pm to 5am
    - Regular phishing exercises
    - All staff who have access to the schools' MIS undertake NCSC Cyber Security training
    - A cyber response plan in place
    - Offline back ups
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 10)

21. Transparency and Privacy Notices – See Appendix 1

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The School's privacy notices are tailored to suit the data subject and set out information about how the School use their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

22. Record Keeping

The School are required to keep full and accurate records of our data processing activities. These records include:

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the School's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

23. Disposal of Records

See the school's Management of Records Policy

24. Personal Data Breaches

The UK GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. Please refer to our Data Breach policy. This is available on the school's shared drive.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches (who is The Operations Manager (Bentley Wodo)/the School Business Manager (Aylward) or your DPO.

25. Training

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The school will carry out adequate training with all staff annually.

.

26. Monitoring arrangements

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

27. Links with other policies

This data protection policy is linked to our:

Bentley Wood Trust Freedom of Information Publication Scheme

- Bentley Wood Trust School Management of Records Policy
- Bentley Wood Trust
- ICT and Online safety
- CCTV Policy
- Child Protection Policy and Procedures (Safeguarding)
- Bentley Wood Trust Data Breach Policy

Appendix 1: Privacy Notices

Bentley Wood Trust

Privacy notice – How we Use Student Information

Under data protection law, individuals have a right to be informed about how each school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about Students. It is based on the Department for Education's model privacy notice for Students amended to reflect the way we use data in our schools.

We, Bentley Wood Trust, are the 'data controller' for the purposes of data protection law. Our Data Protection Officers are Naseema Akbar (Aylward Primary), Louise Kelly (Bentley Wood) (see 'Contact us' below).

The categories of student information we process include:
Personal data that we may collect, use, store and share (when appropriate) about Students includes, but is not restricted to:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address, identification documents)
- Results of internal assessments and externally set examinations
- Student and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or
- Special educational needs (including needs and ranking)
- Behavioural information (such as exclusions and any alternative provision put in place)
- Details of any medical and administration, including physical and mental health, Doctors information, allergies, medication and dietary requirements
- Attendance information (such as sessions attended, number of absences, absence reasons, and any previous schools attended)
- Safeguarding information (such as court orders and professional involvement)
- Educational Visit records
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school
- Biometric data used as part of the school's cashless payment system

We may also hold data about Students that we have received from other organisations, including other schools, local authorities and the Department for Education.

This list is not exhaustive, to access the current list of categories of information we process please see each individual schools' website for current privacy notices.

Why we collect and use student information:
We use this data to:

1. Support student learning
2. Monitor and report on student attainment and progress
3. Provide appropriate pastoral care
4. Assess the quality of our services
5. Keep children safe (food allergies, or emergency contact details)
6. Comply with the law regarding data sharing (such as, meeting the statutory duties placed upon us for DfE data collections).
7. Administer admissions waiting lists
8. Carry out research
9. Protect student welfare

Our legal basis for using this data

We only collect and use Students' personal data when the law allows us to. Under the General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing student information are:
for the purposes of **(1), (2), (3), (4), (7), (8) and (9)** in accordance with the legal basis of Public task: collecting the data is necessary to perform tasks that schools are required to perform as part of their statutory function

- for the purposes of **(5)** in accordance with the legal basis of Vital interests: to keep children safe (food allergies, or medical conditions)
- for the purposes of **(6)** in accordance with the legal basis of Legal obligation: data collected for DfE census information
- Section 537A of the Education Act 1996
- the Education Act 1996 s29(3)
- the Education (School Performance Information) (England) Regulations 2007
- regulations 5 and 8 School Information (England) Regulations 2008
- the Education (Pupil Registration) (England) (Amendment) Regulations 2013

In addition, concerning any special category data:

- • conditions a, b, c and d of UK GDPR - Article 9

Less commonly, we may also process Students' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use Students' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using Students' personal data overlap, and there may be several grounds which justify our use of this data.

How we collect student information

We obtain student information via registration forms at the start of each academic year. In addition, when a child joins us from another school we are sent a secure file containing relevant information. Student data is essential for the schools' operational use. Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with UK GDPR we will inform you at the point of collection, whether you are required to provide certain student information to us or if you have a choice in this.

At Bentley Wood High School, we also use you information as part of an automated(i.e electronically operated) recognition system. This is for the purposes of paying for items in the school canteen

How we store student data

We keep personal information about Students while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Please see our School Records Management Policy, available from each school's website, which sets out how long we keep information about students.

Who we share student information with

Where it is legally required, or necessary (and it complies with data protection law) we routinely share personal information about students with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education – to meet our legal obligations under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.
- The Student's family and representatives
- Educators and examining bodies – as part of delivering the curriculum.
- Ofsted – to meet regulatory requirements around inspections.
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations – to enable us to provide services to students such as the catering provision
- Our auditors - to meet the requirements of the Academies Financial Handbook and the Academies

Accounts Direction.
- Health authorities - to enable them to provide services and support to Students.
- Police forces, courts, tribunals
- Health and social welfare organisations - to enable them to provide services and support to Students.
- Professional advisers and consultants - to enable them to provide the service we have contracted them for
- Charities and voluntary organisations - to enable them to provide services and support to Students.
- Youth support services (students aged 13+)
- Schools that students attend after leaving us

Why we regularly share student information

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

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student 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 / student once he/she reaches the age 16.

Students aged 16+

We will also share certain information about students 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

Data is securely transferred to the youth support service via a secure file transferring system and is stored within local authority software.

For more information about services for young people, please visit our local authority **(**Harrow) website http://www.harrow.gov.uk/

Department for Education

We are required to share information about our students with the Department for Education (DfE) either directly or via our local authority for the purpose of data collections, under:

- Section 537A of the Education Act 1996
- the Education Act 1996 s29(3)
- the Education (School Performance Information) (England) Regulations 2007
- regulations 5 and 8 School Information (England) Regulations 2008
- the Education (Pupil Registration) (England) (Amendment) Regulations 2013

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.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

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

Other rights
Under data protection legislation, parents and students have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Withdraw consent by writing to us if we rely on your consent to justify processing your information,
- a right to seek redress, either through the ICO, or through the courts

How to Raise a Concern
If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with the below in the first instance:

Aylward Primary School **Louise Kelly** **Headteacher** **Aylward Primary School** **Pangbourne Drive** **Stanmore** **HA7 4RE** **Telephone: 020 8958 9202**	**Bentley Wood High School** **Naseema Akbar** **Headteacher** **Bentley Wood High School** **Clamp Hill,** **Stanmore,** **HA7 3JW** **Tel 0208 954 3623**

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the above, then you can contact the DPO on the details below: -
Data Protection Officer: Judicium Consulting Limited
Address 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

How Government uses your data
The student data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or student progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools
The National Pupil Database (NPD)
Much of the data about students in England goes on to be held in the National Pupil Database (NPD).
The NPD is owned and managed by the Department for Education and contains information about students 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.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing by the Department
The law allows the Department to share students' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

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

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 students per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided student information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

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

The Bentley Wood Trust (comprising of Bentley Wood High School & Aylward Primary School) is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

Successful candidates should refer to our privacy notice for staff for information about how their personal data is stored and collected.

Who Collects This Information

The Bentley Wood Trust is a "data controller." This means that we are responsible for deciding how we hold and use personal information about you.

We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

The Categories Of Information That We Collect, Process, Hold And Share

We may collect, store and use the following categories of personal information about you up to the shortlisting stage of the recruitment process: -

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment including proof of right to work in the UK, information entered on the application form, CV, qualifications;
- Details of your employment history including job titles, salary and working hours;
- Information regarding your criminal record as required by law to enable you to work with children;
- Details of your referees and references;
- Details collected through any pre-employment checks including online searches for data;
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs.

We may also collect information after the shortlisting and interview stage in order to make a final decision on where to recruit, including criminal record information, references, information regarding qualifications. We may also ask about details of any conduct, grievance or performance issues, appraisals, time and attendance from references provided by you.

How We Collect This Information

- We may collect this information from you, your referees, your education provider, relevant professional bodies the Home Office and from the DBS.

How We Use Your Information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances: -

- Where we need to take steps to enter into a contract with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.
- Where you have provided your consent for us to process your personal data.

Generally the purpose of us collecting your data is to enable us to facilitate safe recruitment and determine suitability for the role. We also collect data in order to carry out equal opportunities monitoring and to ensure appropriate access arrangements are put in place if required.
If you fail to provide certain information when requested, we may not be able to take the steps to enter into a contract with you (for example if incorrect references are provided), or we may be prevented from complying with our legal obligations (such as to determine suitability to work with children).
We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

How We Use Particularly Sensitive Information

Sensitive personal information (as defined under the UK GDPR as "special category data") require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances: -

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring;
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.
Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

Sharing Data

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.
These include the following: -

- Academic or regulatory bodies to validate qualifications/experience (for example the teaching agency);
- Referees;
- Other schools;
- DBS; and
- Recruitment and supply agencies.

We may also need to share some of the above categories of personal information with other parties, such as HR consultants and professional advisers. Usually information will be anonymised but this may not always be possible. The recipients of the information will be

bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

How long we keep your information will depend on whether your application is successful and you become employed by us, the nature of the information concerned and the purposes for which it is processed. Full details on how long we keep personal data for is set out in our data retention policy.

Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Your Rights Of Access, Correction, Erasure And Restriction

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances by law you have the right to: -

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Headteacher in writing. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right To Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Headteacher. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

How To Raise A Concern

We hope that the Headteacher can resolve any query you raise about our use of your

information in the first instance.
We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolve by the Headteacher, then you can contact the DPO on the details below: -
Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell
You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

The Bentley Wood Trust contact details are as follows:-

Bentley Wood High School **Naseema Akbar (Headteacher)** **Clamp Hill,** **Stanmore,** **HA7 3JW** **Tel 020 8954 6323**	**Aylward Primary School** **Louise Kelly (Headteacher)** **Pangbourne Drive** **Stanmore** **HA7 4RE** **Telephone: 020 8958 9202**

Privacy Notice for Governors and Volunteers

The Bentley Wood Trust

The Bentley Wood Trust is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).
Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement.
The GDPR as it continues to apply in the EU is known as EU GDPR.
It applies to governors and volunteers.

Who Collects This Information

The Bentley Wood Trust is a "data controller." This means that we are responsible for deciding how we hold and use personal information about you.
We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.
It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

The Categories of Information That We Collect, Process, Hold and Share

We may collect, store and use the following categories of personal information about you: -

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Education details;
- DBS details;
- Employment details;
- Information about business and pecuniary interests;
- Information acquired as part of your application to become a governor;
- Criminal records information as required by law to enable you to work with children;
- Information about your use of our IT, communications and other systems, and other monitoring information;
- Photographs;
- Images captured by the School's CCTV system;
- Video recordings capture by the School's video conferencing platform;
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;
- Details in references about you that we give to others.

How We Collect This Information

We may collect this information from you directly, from the DBS, other employees and professionals we may engage, automated monitoring of our websites and other technical systems such as our computer networks and connects, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.
A majority of the information that we collect from you is mandatory, however there is

some information that you can choose whether or not to provide it to us. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How We Use Your Information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances: -

- Where you have provided your consent;
- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation and under statutory codes of practice);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

We need all the categories of information in the list above primarily to allow us to comply with our legal obligations and to enable us as a School to perform our public task. Please note that we may process your information without your knowledge or consent, where this is require or permitted by law.

The situations in which we will process your personal information are listed below: -

- To determine appointment and suitability as a governor;
- To deal with election of governors;
- To comply with safeguarding obligations;
- To provide details on our website or online databases about governors;
- To communicate with third parties and other stakeholders to the School;
- For business management and planning purposes (including accounting, budgetary and health and safety purposes;
- For financial purposes (such as expenses);
- To deal with any complaints/investigations as required;
- When you sit on a panel or committee, name and comments as well as decisions made;
- To send communications in your role as governor;
- For education, training and development requirements;
- In order to review governance of the School;
- In order to comply with any legal dispute or any legal obligations;
- In order to comply with regulatory requirements or health and safety obligations;
- To ensure system security, including preventing unauthorised access to our networks;
- To monitor use of our systems to ensure compliance with our IT processes;
- To receive advice from external advisors and consultants;
- To liaise with regulatory bodies (such as the DfE, DBS); and
- Dealing with termination of your appointment;

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide certain information when requested, we may be prevented from complying with our legal obligations (such as to ensure health and safety). Where you have provided us with consent to use your data, you may withdraw this consent at any time.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

How We Use Particularly Sensitive Information

Sensitive personal information (as defined under the UK GDPR as "special category data") require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances: -

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in the following circumstances: -

- Where we have notified you of the decision and given you 21 days to request a reconsideration;
- Where it is necessary to perform the contract with you and appropriate measures are put in place to safeguard your rights; or
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Sharing Data

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following: -

- Government departments or agencies
- The Local Authority
- Suppliers and Service providers
- Professional advisors and consultants
- The Department for Education
- Law enforcement
- Other schools within the federation/trust
- Support services;
- DBS.

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the School

only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.
To determine the appropriate retention period for personal data, the School considers the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for processing the personal data, whether we can fulfil the purposes of processing by other means and any applicable legal requirements.
Once you are no longer a governor or volunteer of the school we will retain and securely destroy your personal information in accordance with our data retention policy.

Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.
We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Your Rights of Access, Correction, Erasure and Restriction

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.
Under certain circumstances by law you have the right to: -

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please submit the request in writing.

Aylward Primary School

Louise Kelly
Headteacher
Aylward Primary School
Pangbourne Drive
Stanmore
HA7 4RE

Telephone: 020 8958 9202

Bentley Wood High School

Naseema Akbar
Headteacher
Bentley Wood High School
Clamp Hill,
Stanmore,
HA7 3JW

Tel 0208 954 6323

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Naseema Akbar or Mrs Louise Kelly. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

How to Raise a Concern

We hope that Naseema Akbar or Louise Kelly can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by Naseema Akbar or Louise Kelly then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

Changes to This Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Privacy Notice for Visitors & Contractors

The Bentley Wood Trust (comprising of Bentley Wood High School & Aylward Primary School) is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your visit with us, in accordance with the UK General Data Protection Regulation (UK GDPR).
Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.
This notice applies to all current and former visitors and contractors.

Who Collects This Information

The Bentley Wood Trust is a "data controller." This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.
This notice does not form part of a contract to provide services and we may update this notice at any time.
It is important that you read this notice, with any other policies mentioned within this privacy notice, so you understand how we are processing your information and the procedures we take to protect your personal data.

Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

Categories of Visitor Information we Collect, Process, Hold and Share

We process data relating to those visiting our school (including contractors). Personal data that we may collect, process, hold and share (where appropriate) about you includes, but is not restricted to:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Criminal records information as required by law to enable you to work with children e.g. DBS checks;
- Information relating to your visit, e.g. your company or organisations name, arrival and departure time, car number plate;
- Information about any access arrangements you may need;
- Photographs for identification purposes for the duration of your visit;
- CCTV footage captured by the school.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious or philosophical beliefs
- Information about your health, including any medical conditions.

How We Collect This Information

We may collect this information from you, the Home Office, the DBS, other professionals we may engage (e.g. to advise us generally), our signing in system, automated monitoring of our websites and other technical systems such as our computer networks and connections, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.

How We Use Your Information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.
- When you have provided us with consent to process your personal data.

We need all the categories of information in the list above primarily to allow us to perform our contract with you, with your consent and to enable us to comply with legal obligations.

The situations in which we will process your personal information are listed below:

- Ensure the safe and orderly running of the school;
- To manage our workforce and those deployed on site;
- Personnel management including retention
- In order to manage internal policy and procedure;
- Complying with legal obligations;
- Carry out necessary administration functions to allow visitors and contractors on site;
- To monitor and manage access to our systems and facilities in order to protect our networks and for the purposes of safeguarding;
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and will explain the legal basis which allows us to do so.

How We Use Particularly Sensitive Information

Sensitive personal information (as defined under the UK GDPR as "special category data") require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring;
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We

will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Sharing Data

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following:

- the Department for Education (DfE);
- Ofsted;
- other schools within the Trust
- Law enforcement officials such as police, HMRC;
- LADO;
- Professional advisors such as lawyers and consultants;
- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority; and
- DBS.

Information will be provided to those agencies securely or anonymised where possible. The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

We will retain and securely destroy your personal information in accordance with our data retention policy. This can be obtained from the School Office.

Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be obtained from the School Office.

Your Rights Of Access, Correction, Erasure And Restriction

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Under certain circumstances by law you have the right to:

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.

- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact Headteacher in writing. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

Right To Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Headteacher. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

How To Raise A Concern

We hope that the Headteacher can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolve by the Headteacher, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

The Bentley Wood Trust contact details are as follows:-

Bentley Wood High School **Naseema Akbar (Headteacher)** **Clamp Hill,** **Stanmore,** **HA7 3JW** **Tel 020 8954 6323**	**Aylward Primary School** **Louise Kelly (Headteacher)** **Pangbourne Drive** **Stanmore** **HA7 4RE** **Telephone: 020 8958 9202**

Privacy notice for staff (How we use workforce information)

Under data protection law, individuals have a right to be informed about how our schools uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.
This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our schools. It is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in our schools.
We, the Bentley Wood Trust, are the 'data controller' for the purposes of data protection law.

Our Data Protection Officers are Naseema Akbar (Aylward Primary), Clive Westall (Bentley Wood) (see 'Contact us' below).

The personal data we hold, process and share
We process data relating to those we employ, or otherwise engage, to work at our schools. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Personal information (such as, Name, contact details, employee/teacher number)
- Characteristics information (such as, date of birth, gender, marital status, ethnicity)
- Next of kin and emergency contact numbers
- Contract information (such as start date, hours worked, post, role, salary, timesheets, annual leave, pension and benefits information)
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- DBS information to demonstrate compliance with Keeping Children Safe in Education (actual certificates are not retained).
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data (such as number of absences and reason)
- Accident reporting and records relating to accident/injury at work
- Copy of driving license where authorised School Minibus Driver.
- Photographs
- CCTV footage

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

This list is not exhaustive, to access the current list of categories of information we process please see each individual schools' website for current privacy notices.

Why we collect and use workforce information
The purpose of processing this data is to help us run each school, including to:

- Enable you to be paid
- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Comply with employment law obligations

- Facilitate safe recruitment, as part of our statutory safeguarding obligations towards students
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body
- Contacting your or your nominated next of kin in emergencies

Our lawful basis for processing this data
We only collect and use staff personal data when the law allows us to. Under the General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing staff information are:

We process this information under the Employment Rights Act 1996, the Trade Union and Labour Relations (Consolidation) Act 1992, The Agency Workers Regulations 2010, the Employment Acts 2002 and 2008, the Employee Relations Act 1999, the Equality Act 2010, and all other relevant employment related legislation.
We may also process this information with consent where appropriate and to establish, exercise and defend legal claims.

Most commonly, we use it where we need to:
- Fulfil a contract we have entered into with you
- Comply with a legal obligation including the submission of the School Workforce Census to the DfE.
- Carry out a task in the public interest
- Where it is needed in the public interest or for official purposes
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests
- When you have provided us with consent to process your personal data

Less commonly, we may also use personal information about you where:
- You have given us consent to use it in a certain way, for example accessing staff benefits such childcare vouchers.
- We need to protect your vital interests (or someone else's interests)

In addition, concerning any special category data:
- • conditions a, b, c and d of GDPR - Article 9

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using staff personal data overlap, and there may be several grounds which justify our use of this data.

Collecting workforce information
We collect personal information via a number of methods, such as, application and recruitment forms, annual data collection sheets, medical forms and adhoc written notifications of updates to information. This could also be through the Home Office, our pension providers, medical and occupational health professions we engage with, your trade union, and even other employees. Information is also collected through CCTV, access control systems and any IT system the school has in place.

Workforce data is essential for each school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with UK GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information
We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.
Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our School Records Management Policy available on each School's website.

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

Where it is legally required, or necessary (and it complies with data protection law) we may regularly share personal information about you with:

Department for Education
The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under:

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

For more information, please see 'How Government uses your data' section.

- Harrow Council - We are required to share information about our workforce members with our local authority under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- Your family or representatives
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll, communication systems
- Financial organisations including the Trusts bankers to enable processing of payroll.
- Our auditors - to meet the requirements of the Academies Financial Handbook and the Academies Accounts Direction.
- Trade unions and association
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies
- Third Parties for Occupational Heath Purposes

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

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

How to Raise a Concern
If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with the below in

the first instance:

Aylward Primary School **Louise Kelly** **Headteacher** **Aylward Primary School** **Pangbourne Drive** **Stanmore** **HA7 4RE** **Telephone: 020 8958 9202**	**Bentley Wood High School** **Naseema Akbar** **Headteacher** **Bentley Wood High School** **Clamp Hill,** **Stanmore,** **HA7 3JW** **Tel 0208 954 3623**

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the above, then you can contact the DPO on the details below: -
Data Protection Officer: Judicium Consulting Limited
Address 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

How 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

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

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

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

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

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

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

Appendix 2 – Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School are undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A data subject has the right to be informed by the School of the following: -

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the School's sources of information obtained;

(g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

(h) Other supplementary information.

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, we will have only one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay. Failure to deal with a SAR within that period could leave us open to the possibility of being fined by the ICO.

All staff must be aware of the potential for receiving a SAR and the importance of dealing with such as request as a matter of urgency.

Anyone within the School may receive a SAR. It does not need to be made to a nominated person or even to a person responsible for dealing with either the data subject or information of that type. It will be equally as valid if sent to anyone within the school.

If you receive a SAR, please contact the School Business Manager (Aylward)/Operations Manager (Bentley Wood) A request for information does not need to mention that it is a SAR provided that it is clear that it is an individual asking for their own personal data. There is no specified wording and it does not have to be on an official form. A SAR does not need to be in writing and can be made verbally, by post, by email or even using social media where relevant.

How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the School process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text, social media) or verbally (e.g., during a telephone conversation or meeting). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

How to Make a Data Subject Access Request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

If a request is made verbally, we will ensure we follow this up with something in writing to confirm what has been requested and outline the timeframe for dealing with the request.

What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the School Business Manager (Aylward)/Operations Manager (Bentley Wood) who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual. If ever in doubt, please refer the request to the School Business Manager (Aylward)/Operations Manager (Bentley Wood)

Acknowledging the Request

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);
- further clarification about the requested information if it is not clear what information is required;
- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

Verifying the Identity of a Requester or Requesting Clarification of the Request

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request,

evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the school will be unable to comply with the request if they do not receive the additional information.

Requests Made by Third Parties or on Behalf of Children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee For Responding to a SAR

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received. Where the school may be required to get consent from a pupil, the time period will not start until consent is received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School Closure Periods

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the school will be closed other than to site staff. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Company rectifies, erases or restricts the processing of his personal data; or

- to object to its processing;
- to lodge a complaint with the ICO;
- where the personal data has not been collected from the individual, any information available regarding the source of the data;
- any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the School is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

How to Locate Information

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the School may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- safeguarding systems (such as CPOMS, MyConcern);
- MIS system (such as SIMS, Bromcom, Arbor);
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The School should search these systems using the individual's name, initials, employee number or other personal identifier as a search determinant.

Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the School receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The School do not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The school can refuse to comply with a request if the request in certain circumstances. These include:

- Where the SAR is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature;
- To avoid obstructing an official or legal inquiry, investigation or procedure;
- To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- To protect public security;
- To protect national security;
- To protect the rights and freedoms of others.

In the event that you have concerns about supplying the information, you must always refer the matter to the School Business Manager (Aylward)/Operations Manager (Bentley Wood) who will make the decision on our behalf.

In the event that we decide not to comply with the SAR, then the data subject must be informed, without undue delay (and in all cases within one month of receipt of the request), of:

- The reasons we are not taking action;
- That they have a right to make a complaint to the ICO or another supervisory authority; and
- That they are entitled to seek to enforce their right through a judicial remedy.

If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

Record Keeping

A record of all subject access requests shall be kept by the the School Business Manager (Aylward)/Operations Manager (Bentley Wood). The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

Appendix 2 – Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ∆ Birth certificate
- ∆ Driving licence
- ∆ Passport
- ∆ An official letter to my address

Personal Information

If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records:

If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ∆ Birth certificate
- ∆ Driving licence
- ∆ Passport
- ∆ An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ∆ Letter of authority
- ∆ Lasting or Enduring Power of Attorney
- ∆ Evidence of parental responsibility
- ∆ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- Δ Receive the information by post*
- Δ Receive the information by email
- Δ Collect the information in person
- Δ View a copy of the information only
- Δ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to:

Aylward Primary School: Marion Tam tamm@aylward.harrow.sch.uk

Bentley Wood High School: Paola Boyadjian pboyadjian@bentleywood.harrow.sch.uk