Woodpecker Court
Wigmore lane Eythorne Kent CT15 4BF
Tel: 01304 830958
Email: dmeehan@woodpeckercourt.com
Registered company: 9629678 registered in England & WalesVAT
registration number: 218990574

Woodpecker Court UK GDPR and Data Protection Policy

V3

Version control

Version	Reviewed by	Future Review date	Comments	Approved by board
V1	ES	Apr 2022	Policy written and implemented	23/04/2020
V2	ES	Jul 2023	Policy reviewed and updated	15/07/2021
V3	MAN	June 2024	Version control added. Policy reviewed and updated.	15/06/2023

General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone whohandles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files orelectronically.

Policy Objectives

Woodpecker Court as the Data Controller will comply with its obligations under the UK GDPR and DPA. The provision is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rightsunder the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered,used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the UK GDPR, therefore it is imperative thatthe provision and all staff comply with the legislation.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the UK GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

Woodpecker Court collects a large amount of personal data every year including: student records, staff records, names and addresses of those requesting prospectuses, examinationmarks, references, fee collection as well as the many different types of research data used by the provision. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Principles

The principles set out in the UK GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner **(lawfulness, fairness and transparency)**
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **(purpose limitation)**
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed **(data minimisation)**
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay **(accuracy).**
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed **(storage limitation)**
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data **(integrity and confidentiality).**

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA unless thatcountry or territory ensures an adequate level of protection for the rights and freedoms ofdata subjects in relation to the processing of personal data as determined by the EuropeanCommission or where the organisation receiving the data has provided adequate safeguards[2].

2 These may be provided by a legally binding agreement between public authorities or bodies,standard data protection clauses provided by the ICO or certification under an approved mechanism.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer datawhere the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) forthat processing must be selected:

- Processing is necessary for the performance of a task carried out in the publicinterest or in the exercise of official authority vested in the provision
- Processing is necessary for the performance of a contract to which the data subjectis party, or in order to take steps at the request of the data subject prior to enteringinto a contract
- Processing is necessary for compliance with a legal obligation to which the datacontroller is subject
- Processing is necessary in order to protect the vital interests of the data subject orof another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by thedata controller or by a third party[3]

3 The UK GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that wherethere are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statementor positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate fromthose other matters

Data subjects must be easily able to withdraw consent to processing at any time andwithdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both thepurposes of the processing and the lawful basis for it in the provision's relevant privacynotice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the provision's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impactis identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data')is prohibited[4] unless a lawful special condition for processing is identified.

4 UK GDPR, Article 9

Sensitive personal information is data which reveals racial or ethnic origin, political opinions,religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:

(a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the provision or the datasubject

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent

(d) the processing is carried out in the course of its legitimate activities withappropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-unionaim

(e) the processing relates to personal data which are manifestly madepublic by the data subject

(f) the processing is necessary for the establishment, exercise or defence oflegal claims

(g) the processing is necessary for reasons of substantial public interest

(h) the processing is necessary for purposes of preventative or occupationalmedicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services

(i) the processing is necessary for reasons of public interest in the area ofpublic health.

The provision's privacy notice(s) set out the types of sensitive personal information that itprocesses, what it is used for, the lawful basis for the processing and the special conditionthat applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individualhas been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the provision can rely on another legal basis of processing, explicit consent is usuallyrequired for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the provision can demonstrate compliance with the UK GDPR.

Automated Decision Making

Where the provision carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usuallybe required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision- making, including profiling. The provision must as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processingand that the data subject may request the provision to reconsider or take a new decision. Ifsuch a request is received staff must contact the DPO as they must reply within 21 days.

Data Protection Impact Assessments (DPIA)
All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the provision's processes must embed privacy considerations and incorporateappropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference tothe DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidanceand once complete, refer the finalised document to the DPO for sign off.

Documentation and records
Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfermechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.

As part of the provision's record of processing activities the DPO will document, or link todocumentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information;
- DPIAs and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it isnecessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with theRetention Schedule and, if not, the reasons for not following the policy.

The provision should conduct regular reviews of the personal information it processes andupdate its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities

- Reviewing policies, procedures, contracts and agreements to address retention,security and data sharing.

Privacy Notice

The provision will issue privacy notices as required, informing data subjects (or their parents, depending on age of the student, if about student information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the UK GDPR including the identity of the DPO, how and why the provision will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. The provision must also check that the data was collected by the third party in accordance with the UK GDPR and on a basis which is consistent with the proposed processing of the personal data.

The provision will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The provision will issue a minimum of two privacy notices, one for student information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

Purpose Limitation
Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data minimisation
Personal data must be adequate, relevant and limited to what is necessary in relation to thepurposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The provision maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights
Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed
- (see the relevant privacy notice)

- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request

- To have data corrected if it is inaccurate or incomplete

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')

- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the provision no longer need the personal information, but you require the data to establish, exercise or defend a legal claim

- To restrict the processing of personal information temporarily where you do not think it is accurate (and the provision are verifying whether it is accurate), or where you have objected to the processing (and the provision are considering whether the provision's legitimate grounds override your interests)

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

- To withdraw consent to processing at any time (if applicable)

- To request a copy of an agreement under which personal data is transferred outside of the EEA.

- To object to decisions based solely on automated processing, including profiling

- To be notified of a data breach which is likely to result in high risk to their rights and obligations

- To make a complaint to the ICO or a Court.

Individual Responsibilities
During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The provision expects staff to help meetits data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not provision staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the provision's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the provision's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security
The provision will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their provision's acceptable usage policy.

The provision will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the

effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity** and **availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the provision has implemented and maintains in accordance with the UK GDPR and DPA.

Where the provision uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the provision
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the provision and under a written contract
- the organisation will assist the provision in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the provision as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the provision with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the provision immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information
Personal data will be kept securely in accordance with the provision's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:
http://www.kelsi.org.uk/ data/assets/word_doc/0012/60213/InformationManagementTo olkitforSchoolsv4-2.docx

Personal information that is no longer required will be deleted in accordance with the

Provision's Record Retention Schedule.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The provision must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The provision must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Principal immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the provision's agreed breach reporting process.

Training

The provision will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

The provision takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the provision and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the provision's procedures and this action may result in dismissal for gross misconduct. If a non- employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the provision's DPO.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the UK GDPR or DPA.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

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. profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the UK GDPR. The provision is the Data Controller of all personal data relating to its students, parents and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the UK GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not justaction).

General Data Protection Regulation (UK GDPR): General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the UK GDPR.

Personal data: is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal 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 breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the provision collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, provision workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination orotherwise making available, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body whichprocesses personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectlyidentifies an individual with one or more artificial identifiers or pseudonyms so that theperson, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions,sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

Woodpecker Court
Wigmore lane Eythorne Kent CT15 4BF Tel:
01304 830958 Mobile: 07720 800391
Email: dmeehan@woodpeckercourt.com
Registered company: 9629678 registered in England & Wales
VAT registration number: 218990574

Woodpecker Court Privacy notice for job applicants

Document Owner and Approval

Woodpecker Court is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff on the shared drive.

Signature: Date:

Change History Record

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	06.05.18
2	Updated for UK GDPR and international transfers outside of the UK	06.05.21
3	Updated to include reference to online searches	20.07.22

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

Woodpecker Court 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 policies mentioned within this privacy notice. This will assist you with understanding how we process 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 Information 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, by searching online resources, from 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, or we may be prevented from complying with our legal obligations.

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.

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.

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.
- Our Local Authority in order to meet our legal obligations for sharing data with it;
- Other organisations (Woodpecker Wood)

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 Provision 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.
Once we have finished recruitment for the role you applied for, we will then store your information in accordance with our Retention Policy. This can be found on the shared drive.

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 found on the shared drive.

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 Matthew Anderson 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 Matthew Anderson. 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 Matthew Anderson 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 Matthew Anderson, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
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.

Woodpecker Court
Wigmore lane Eythorne Kent CT15 4BF Tel:
01304 830958 Mobile: 07720 800391
Email: dmeehan@woodpeckercourt.com
Registered company: 9629678 registered in England & Wales
VAT registration number: 218990574

Woodpecker Court
Privacy notice for staff

Document Owner and Approval

Woodpecker Court is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff on the shared drive.

Change History Record

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	06.05.18
2	Updated for UK GDPR and international transfers outside of the UK	06.05.21

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 all current and former employees, workers and contractors.

Who Collects this Information?

Woodpecker Court 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 with any other policies mentioned within this privacy notice, so that 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 Information 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;
- Information collected during the recruitment process that we retain during your employment including references, proof of right to work in the UK, application form, CV, qualifications;
- Employment contract information such as start dates, hours worked, post, roles;
- Education and training details;
- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information;
- Details of any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- Information in your sickness and absence records such as number of absences and reasons(including sensitive personal information regarding your physical and/or mental health);
- Criminal records information as required by law to enable you to work with children;
- Your trade union membership;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals, performance reviews and capability issues;
- Details of your time and attendance records;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Details of your use of business-related social media;
- Images of staff captured by the Provision's CCTV system;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the Provision, you will be notified separately if this is to occur); and
- Details in references about you that we give to other;

- Recordings of staff from the Provision's video conferencing platform (Teams, Zoom, remote lesson obs)
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs.

How we Collect this Information

We may collect this information from you in your application form, but we will also collect information in a number of different ways. This could be through the Home Office, our pension providers, medical and occupational health professionals 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.

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 and to enable us to comply with legal obligations.

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

- To determine recruitment and selection decisions on prospective employees;
- In order to carry out effective performance of the employees contract of employment and to maintain employment records;
- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- Enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management including retention, sickness and attendance;
- Performance reviews, managing performance and determining performance requirements;
- In order to manage internal policy and procedure;
- Human resources administration including pensions, payroll and benefits;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees 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;
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- 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.

Further information on the monitoring we undertake in the workplace and how we do this is available on the shared drive.
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 not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations.

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.

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 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.

We will use this information in the following ways:

- Collecting information relating to leave of absence, which may include sickness absence or family related leave;
- To comply with employment and other laws;
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;
- Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

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

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.
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;
- Prospective Employers;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- LADO;
- Training providers;
- Professional advisors such as lawyers and consultants;

- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority;
- Occupational Health;
- DBS;
- Recruitment and supply agencies; and
- Woodpecker Wood

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.

Retention Periods

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

Once you are no longer a staff member at the provision we will retain and securely destroy your personal information in accordance with our data retention policy. This can be found on the shared drive.

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. Details of these measures are available on the shared drive.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found on the shared drive.

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.

Your Rights of Access, Correction, Erasure and Restriction

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 Matthew Anderson 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 Matthew Anderson. 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.

We hope that Matthew Anderson 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 Matthew Anderson, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

How to Raise a Concern

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.

Woodpecker Court
Wigmore lane Eythorne Kent CT15 4BF
Tel: 01304 830958 Mobile: 07720 800391
Email: dmeehan@woodpeckercourt.com
Registered company: 9629678 registered in England & WalesVAT registration number: 218990574

Woodpecker Court Privacy notice for volunteers, visitors and contractors

Document Owner and Approval

Woodpecker Court is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

Change History Record

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	06.05.18
2	Updated for UK GDPR and international transfers outside of the UK	06.05.21

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.

It applies to all current and former volunteers, visitors and contractors.

Who Collects this Information

Woodpecker Court 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 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 provision.

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 provision;
- 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.

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 organisations (Woodpecker Wood)
- 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.

Retention Periods

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

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 found on the shared drive.

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 Matthew Anderson 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 Matthew Anderson. 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.

We hope that Matthew Anderson 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 Matthew Anderson, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

How to Raise a Concern

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.

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Woodpecker Court
Wigmore lane Eythorne Kent CT15 4BF Tel:
01304 830958 Mobile: 07720 800391
Email: dmeehan@woodpeckercourt.com
Registered company: 9629678 registered in England & Wales
VAT registration number: 218990574

Woodpecker Court Privacy notice for Advisory Board Members

Document Owner and Approval

Woodpecker Court is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

Change History Record

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	06.05.18
2	Updated for UK GDPR and international transfers outside of the UK	06.05.21

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 Advisory Board Members

Who Collects this Information

Woodpecker Court 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 policies referenced in this privacy notice, to be aware of how we process 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 Information 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 an Advisory Board Member;
- 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 Provision's CCTV system;
- Video recordings capture by the Provision's video conferencing platform (Teams, Zoom, Remote monitoring visits)
- 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

The 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.

We may collect this information from you directly, or from a number of third-party sources, such as other employees,

the DBS, technical networks and so on.

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.

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

- To determine appointment and suitability as an Advisory Board Member;
- To deal with election of Advisory Board Members;
- To comply with safeguarding obligations;
- To provide details on our website or online databases about Advisory Board Members;
- To communicate with third parties and other stakeholders to the Provision;
- 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 an Advisory Board Member;
- For education, training and development requirements;
- In order to review governance of the Provision;
- 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;

Further information on the monitoring we undertake in the workplace and how we do this is available in the Advisory Board Members Handbook also UK GDPR and Data Protection Policy.

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. 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:

- Government departments or agencies
- The Local Authority
- Suppliers and Service providers
- Professional advisors and consultants
- The Department for Education
- Law enforcement
- Support services;
- DBS.
- Other organisations (Woodpecker Wood)

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.

Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the Provision 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. Once you are no longer an Advisory Board Member of the provision we will retain and securely destroy your personal information in accordance with our data retention policy. This can be found on the shared drive.

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. Details of these measures are available on the shared drive. You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found on the shared drive.

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 Matthew Anderson in writing.

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 Matthew Anderson. 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 Matthew Anderson 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 Matthew Anderson, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
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.

Woodpecker Court
Wigmore lane Eythorne Kent CT15 4BF Tel:
01304 830958 Mobile: 07720 800391
Email: dmeehan@woodpeckercourt.com
Registered company: 9629678 registered in England & Wales
VAT registration number: 218990574

Woodpecker Court Privacy notice for students and parents

Document Owner and Approval

Woodpecker Court is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with Provision's policy review schedule.

Change History Record

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	06.05.18
2	Updated for UK GDPR and international transfers outside of the UK	06.05.21
3	Added reference to sharing data section about Department for Education request for regular attendance data collection	18.02.22

This privacy notice describes how we collect and use personal information about students, in accordance with the UK General Data Protection Regulation (UK GDPR), section 537A of the Education Act 1996 and section 83 of the Children Act 1989.

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.

Who Collects This Information

Woodpecker Court is a "data controller." This means that we are responsible for deciding how we hold and use personal information about students and parent/carers.

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

Categories of Student Information We Collect, Process, Hold and Share

- Personal information such as name, student number, date of birth, gender, and contact information.
- Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses;
- Characteristics (such as ethnicity, language, nationality, country of birth and free provision meal eligibility);
- Attendance details (such as sessions attended, number of absences and reasons for absence);
- Performance and assessment information;
- Behavioural information (including exclusions);
- Special educational needs information;
- Relevant medical information;
- Special categories of personal data (including ethnicity, relevant medical information, special educational needs information]);
- Images of students engaging in provision activities, and images captured by the Provision's CCTV system;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Financial details;
- Post 16 learning information;
- Recordings of students and/or parent/carers from the provision's video conferencing platform; (google classroom and remote invigilation, speaking listening and communication assessments

Collecting this Information

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

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.

How We Use Your Personal Information

We hold student data and use it for:

- Student selection (and to confirm the identity of prospective students and their parent/carers);
- Providing education services and extra-curricular activities to students, and monitoring students' progress and educational needs;
- Informing decisions such as the funding of provisions;
- Assessing performance and to set targets for provisions;
- Safeguarding students' welfare and providing appropriate pastoral (and where necessary medical) care;
- Support teaching and learning;
- Giving and receive information and references about past, current and prospective students, and to provide references to potential employers of past students;
- Managing internal policy and procedure;
- Enabling students to take part in assessments, to publish the results of examinations and to record student achievements;
- To carry out statistical analysis for diversity purposes;
- Legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with legal obligations and duties of care;
- Enabling relevant authorities to monitor the provision's performance and to intervene or assist with incidents as appropriate;
- Monitoring use of the provision's IT and communications systems in accordance with the provision's IT security policy;
- Making use of photographic images of students in provisions publications, on the provision website and on social media channels;
- Security purposes, including CCTV; and
- Where otherwise reasonably necessary for the provision's purposes, including to obtain appropriate professional advice and insurance for the provision.
- To provide support to students after they leave the provision

The Lawful Bases on which we use this Information

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

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and
- The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: https://www.gov.uk/education/data-collection-and-censuses-for-provisions.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is required or permitted by law.

Sharing Data

We may need to share your data with third parties where it is necessary. There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it's the only way we can make sure you stay safe and healthy or we are legally required to do so.
We share student information with:

- the Department for Education (DfE) - on a statutory basis under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013;

- Ofsted;
- Other Provisions that students have attended/will attend;
- NHS;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- Local Authority Designated Officer;
- Professional advisors such as lawyers and consultants;
- Support services (including insurance, IT support, information security);
- Providers of learning software such as Edukey
- The Local Authority.
- The information sharing agreement
- Other organisations (Woodpecker Wood)

Recently the Department for Education have requested more regular data sharing on student attendance to help support those vulnerable and to assist with intervention strategies. Further information on how the Department for Education collects this data will be made available on the Provision website.

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 do not share information about our students with anyone without consent unless otherwise required by law.

Why we Share this Information

For example, we share students' data with the DfE on a statutory basis which underpins provision funding and educational attainment. To find out more about the data collection requirements placed on us by the DfE please go to https://www.gov.uk/education/data-collection-and-censuses-for-provisions.

Storing Student Data

The Provision keep information about students on computer systems and sometimes on paper.

Except as required by law, the Provision only retains information about students for as long as necessary in accordance with timeframes imposed by law and our internal policy.

Full details on how long we keep personal data for is set out in our data retention policy, this can be found on the shared drive.

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 limited circumstances.
Students will not be subject to automated decision-making unless we have a lawful basis for doing so and we have notified you.

Retention Periods

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

Information about how we retain information can be found in our Data Retention policy. This document can be found on the shared drive.

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).

The Information Sharing Agreement

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.
We must provide the students' name, the parent/carers' name(s), and any further information relevant to the support service's role.

This enables them to provide services as follows:

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

A parent/carer or guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the young person/ student once he/she reaches the age 16. For more information about services for young people, please visit our local authority website.

The National Student Database

The NPD is owned and managed by the Department for Education and contains information about students in provisions 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 provisions, local authorities, and awarding bodies.

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

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

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

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

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

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

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

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

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

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

Under data protection legislation, parent/carers 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 education record, contact Matthew Anderson.

Requesting Access to your Personal Data

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.
If you want to request information, please see our Subject Access Request policy, for the procedures we take.

Right to Withdraw Consent

In 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 Matthew Anderson. 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.

Contact

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 Matthew Anderson 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 Matthew Anderson, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
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 at https://ico.org.uk/concerns.

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.