Privacy Notice

APRIL WELL LIMITED — Company No. 11924473

Registered office: Unit 39c St Olavs Court Business Center, Lower Road, London, England, SE16 2XB

Director / Legal Representative: Xiaoying Chi

Designated Safeguarding Lead (DSL): Xiaoying Chi

(Deputy DSL: n/a – temporarily covered by the DSL)

24/7 emergency: 07930416543

Email: info@aprilwell.co.uk

This notice is publicly available. It may be shared with parents, agents, partner schools and inspectors on request.

Document Control

Title: Privacy Notice

Owner: Xiaoying Chi, Director / DSL

Approved by: Xiaoying Chi

Document ID: AWP-PN-02

Version: v2.0 (21 October 2026)

Issue date: 21 October 2026

Next review: 21 October 2027 *(or earlier if law/policy changes)*

Status: Public

Distribution: Company website; Student/Parent Handbooks; provided to schools and inspectors on request.

This document is reviewed annually in October and whenever statutory guidance or AEGIS Standards change.

Table of Contents

About us 1
How we collect personal information 2
What personal information we collect about you 2
How we use your personal information 3
4a. How we use your personal information during the recruitment process 4
Who we share your personal information with 6
How we keep your personal information safe 7
How long we keep your personal information for 7
Children's personal information 7
Marketing 9
Links to third-party websites and services 9
Cookies 9
Your legal rights 10
Changes to our Privacy Policy 12

April Well Limited Privacy Notice

When you interact with *April Well Limited*, you trust us to handle your personal information with care. We will always be clear about the ways in which we intend to use your personal information, and the choices and rights you have in relation to it.

This Privacy Policy explains how we collect, use, and store your personal information in relation to your use of this website and the services we offer. It explains what your legal rights are and how you can exercise them. For example, how you can request a copy of the personal information we hold about you. We apply the UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

Please take the time to read this Privacy Policy; it is an important document, and you need to ensure that you understand it. If you have any questions about anything contained in this Policy, please get in touch.

you can write to us at the following address:

April Well Limited
Unit 39c, St Olavs Court Business Center
Lower Road
London
SE16 2XB
United Kingdom

Or send us an email: info@aprilwell.co.uk

About us

We are April Well Limited, referred to throughout this Privacy Policy as “April Well Limited”, “April Well”, “we”, “our”, or “us”.

We are a UK-based education guardianship organisation supporting international students who attend boarding schools and colleges in the United Kingdom. We work in partnership with parents and schools to support student welfare, communication and emergency response. We do not provide routine or long-term homestay accommodation or routine transport services. However, where necessary in clearly defined emergency or exceptional situations, April Well Limited may arrange or coordinate short-term emergency accommodation or transport support in accordance with our safeguarding and emergency procedures.

We are a registered company in England and Wales under company number 11924473 and our registered office is at Unit 39c, St Olavs Court Business Center, Lower Road, London, SE16 2XB, United Kingdom.

For the purposes of this Policy, April Well Limited is the data controller, and we are registered with the Information Commissioner's Office (ICO) under registration number ZB667395.

How we collect personal information

We collect personal information about you whenever you engage with us, apply for a job with us, or use one of our services.

This includes:

- When you use our website
- When you contact us via email, telephone, or post
- When you interact with us on social media platforms e.g. by posting a message on one of our accounts
- When you make a complaint
- When you contact us to exercise one of your legal rights e.g. the right to access your personal information
- When you apply for a job with us
- When you attend a job interview
- When you register to attend an event or training course organised by us
- When you subscribe to our newsletter
- When you apply to use our services

In addition, we may receive personal information about you from other individuals or organisations. For guardianship, sources also include students, parents, agents, schools, healthcare professionals and safeguarding agencies, where necessary and lawful.

This includes:

- When an April Well Limited employee provides your contact details as an emergency contact
- When a job applicant gives your name and contact details as a referee
- When a referee provides information about you during the recruitment process
- When a complainant refers to you in their complaint correspondence

What personal information we collect about you

Personal information means any information that relates to an identified or identifiable individual. The types of personal information we collect about you depends on the nature of your interactions with us.

Depending on the circumstances, we might collect any of the following types of information:

- Your name, address and contact details, including email address and telephone number
- Date of birth
- Financial information, such as payment related information or bank account details
- Technical information, including the type of device you are using to access our website, the Internet Protocol (IP) address, and the browser and operating system being used to connect your device to the internet.
- Information about your visit to our website, including pages you visit and how you use the website
- Details relating to a job application you have made, such as your covering letter and CV, your education and employment history, and any other information relevant to the recruitment process **(please see Section 4a for more information about the recruitment process)**

In some circumstances, we may collect information about you which is sensitive. This is called special category data. We may also collect information about your criminal history. For example, if you apply for a job with us, you may be required to undertake a Disclosure and Barring Service (DBS) check.

Recruitment uses are explained in Section 4a; children's health and ethnicity data are covered under Children's personal information. Special category data requires both an Article 6 basis and an Article 9 condition, such as explicit consent, employment/social protection obligations or substantial public interest safeguarding under DPA 2018 Schedule 1 paragraph 18, only when its conditions are met. Criminal offence/DBS data separately requires Article 10 authorisation and an applicable Schedule 1 condition.

How we use your personal information

We must have a lawful, valid reason for using your personal information. Vital interests may apply where necessary to protect life. Recognised legitimate interest may apply to necessary safeguarding under Article 6(1)(ea) where its statutory conditions are met; it does not remove Article 9 or Article 10 requirements.

The main lawful reasons that we rely on to process your personal information are:

- **Contract performance:** where your personal information is necessary to enter into or perform our contract with you
- **Legal obligation:** where we need to use your personal information to comply with a legal obligation
- **Legitimate interests:** where we use your personal information to achieve a legitimate interest and our reasons for using it outweigh any prejudice to your data protection rights. Our interests include safeguarding students, administering services and recruitment, handling enquiries/complaints and protecting our systems. We balance these against individuals' rights, with particular protection for children.
- **Consent:** where you have given us your consent to use your personal information (you may withdraw your consent at any time)

Contract applies where you are party to the relevant agreement; it is not automatically the basis for a child's data under a parent's contract. Service administration and enquiries normally use legitimate interests, legal duties use legal obligation, and requested marketing uses consent. Safeguarding uses the applicable safeguarding basis above. We may use your personal information to:

- Deal with your enquiries, requests, or complaints
- Send you details about forthcoming events and training courses which you have requested, and we feel would be of interest to you
- Send you communications which you have requested to receive from us
- Process your application for guardianship if you are a parent
- Carry out our obligations under any contracts entered into between you and us, or to meet our legal obligations to regulators, government, and/or law enforcement bodies
- Assess your suitability for a job you have applied for, and to progress your application through the recruitment process **(please see Section 4a for more information about our recruitment process)**
- Better understand how you interact with our website, including pages you visit and areas that are of most interest to you. This is so we can improve our website, the user experience, and target our audience more effectively.

4a. How we use your personal information during the recruitment process

When you apply for a job with us, we will collect and process your personal information. We will only collect personal information that is necessary to assess your suitability for the job you have applied for, to progress your application and keep you updated throughout the process, and to comply with any legal or regulatory obligations.

We collect personal information about you either directly from you or from a third party such as a recruitment agency.

The information we collect may include:

- Your name, address and contact details, including email address and telephone number
- Details about your qualifications (including copies of certificates), skills, experience, and employment history
- Details about any professional memberships you hold
- Information gathered from any interviews you attend
- Information about your current salary level, including benefits and pension entitlements
- Information about your right to work in the UK

In some circumstances, we may collect and process information about you which is sensitive.

This may include:

- Information about your racial or ethnic origin, religious or philosophical beliefs, or sexual orientation for the purpose of our equal opportunities monitoring
- Whether or not you have a disability for which we need to make reasonable adjustments during the recruitment process
- Information about criminal convictions and offences

As part of our recruitment process, we may ask applicants to complete an equal opportunities questionnaire. This is not mandatory; it is entirely your choice as to whether you provide us with this information and there are no adverse consequences if you choose not to.

If you do choose to provide this information to us, we will not make it available to any employees outside of our recruitment team in a way that can identify you. We will use this information to produce and monitor equal opportunities statistics.

If your application for employment is unsuccessful, we will retain your personal information for 6 months. At the end of that period, your personal information will be deleted or securely destroyed, unless we need to retain it for longer to exercise or defend any legal claims, or you have agreed that we can retain your details in our talent pool for a period of 12 months, should any suitable vacancies become available during that time.

If your application for employment is successful, any personal information gathered during the recruitment process will be transferred to your employee file and retained for the duration of your employment with us, plus a period of 6 years following the end of your employment. Different rules apply to safeguarding records. DBS certificate copies are not routinely retained; any justified copy is kept no longer than six months, while necessary check details are recorded (AEGIS 2.8.6).

When an offer of employment is made to you, we will be required to undertake pre-employment checks. For example, we may collect personal information about you from third parties, such as references from current or former employers, information from background check providers, and criminal record checks from the Disclosure and Barring Service (DBS). The timing depends on the check: references may be sought before interview where appropriate, and required checks must be completed before an appointment takes effect. We will tell you before seeking this information.

Once the necessary pre-employment checks have been completed, and the outcomes are satisfactory, we will collect and process additional personal information relating to your employment.

This includes:

- Your bank or building society details, so we can process your salary
- Your emergency contact details, so we know who to contact in the event of an emergency at work

You are under no statutory or contractual obligation to provide your personal information to us during the recruitment process. However, if you do not provide this information, we may not be able to

process your application properly or at all or provide any reasonable adjustments during the recruitment process.

Who we share your personal information with

We will only share your personal information with other organisations where it is lawful for us to do so. When we share your personal information, we will only share the information that is necessary. We will always share information securely and ensure we are giving it to the right recipient.

We may share your personal information with others in the following circumstances:

- Where we are required to do so to comply with a legal or regulatory obligation. For example, we are legally required to provide information about employee income tax contributions to HMRC.
- In an emergency. For example, where we need to protect a person from serious harm.
- Where we have safeguarding concerns about a child, and we need to alert the local authority.
- Where disclosure to a law enforcement authority is legally required or is otherwise necessary and lawful. For example, we might receive a request from the Police for personal information we hold about an individual, to help them investigate a crime.
- To protect our business interests

We may also share your personal information with third parties who provide a service to us. For example, our IT and cloud storage providers, email and communication platforms, and our professional advisers (such as accountants, auditors or legal advisers). We may also share relevant records with AEGIS and its inspectors for accreditation/re-accreditation, where necessary and lawful. For a Gold Standard inspection we obtain and record individuals' permission before supplying their contact details (AEGIS 2.7.6). Sensitive records receive additional safeguards; inspection working copies are kept only as long as needed, without overriding our own safeguarding retention duties.

When we use third parties to process personal information on our behalf, they are required to follow the same rules and information security requirements as us and are not permitted to reuse your personal information for any other purpose. We only share the personal information that is necessary to deliver the service. Where information is transferred outside the UK, including through overseas parents, agents or service providers, we apply the UK GDPR transfer rules where applicable. Restricted transfers require UK adequacy regulations, appropriate safeguards (such as the UK IDTA or Addendum with the required data protection test), or a valid Article 49 exception. You can request details of the countries, recipients, transfer route and a copy of applicable safeguards from info@aprilwell.co.uk.

We will not share your personal information with third parties for marketing purposes and we will never rent or sell your personal information to any other organisation or individual.

How we keep your personal information safe

We have robust technical and operational security measures in place to protect your personal information against unauthorised access or unlawful use.

In addition, we limit access to your personal information to those employees, contractors, and other third parties who have a legitimate business need to know. They will only process your personal information on our strict instructions, and they are subject to a duty of confidentiality.
We maintain internal policies and procedures regarding data protection and confidentiality to ensure that our employees are aware of and understand their responsibilities in relation to your personal information.

We have a robust procedure in place to deal with any suspected personal data breaches. We will notify you and the Information Commissioner's Office (ICO) of any breach within the specified timescales where we are legally required to do so.

You too can play a part in helping to keep your personal information safe. This includes choosing strong passwords, being alert to any fraudulent emails that might appear to be from us (when they are not) and using suitable anti-virus software on your device.

How long we keep your personal information for

We carefully consider how long we keep your personal information for and only keep it for as long as is necessary to fulfil the purpose it was collected for.

We review our data retention periods on a regular basis to ensure that personal information is not held for longer than is necessary. We regularly review the information we hold and delete or securely destroy it when we no longer need it.

In some circumstances, we may anonymise your personal information (so that it can no longer be attributed to you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

Children's personal information

April Well Limited retains students' information in order to fulfil our role as an education guardianship organisation. This may include:

- Name, address, date of birth
- Details of ethnicity

- Contact details, such as phone numbers, email addresses and postal addresses
- School details
- Medical information
- Copies of passports, relevant visa/eVisa or immigration-status evidence, and police-check information only where necessary and lawful
- Details of bank accounts and finances (where relevant to fee payments)
- Information on food preferences, interests and hobbies
- Copies of school reports
- Records of meetings held with students, parents and schools

This information is treated as sensitive information and is stored securely as explained in this notice and is only shared with others on a need-to-know basis. April Well Limited may share information with staff members and school staff. April Well Limited does not provide routine or long-term homestay accommodation. However, where necessary in clearly defined emergency or exceptional situations, April Well Limited may arrange or coordinate short-term emergency accommodation in accordance with its Emergency Procedure and safeguarding policies. Where April Well Limited uses or approves any host family, emergency accommodation adult, external provider or other accommodation arrangement, we may share necessary information with them on a need-to-know basis. April Well Limited may also share information with external agencies where there is a safeguarding concern.

Through this privacy notice, April Well Limited provides information to students and their parents about what records we hold, why we need to hold them and who we might share their information with (for example as part of a multi-agency child protection team). If we are keeping records for child protection reasons, please note that we do not necessarily need to get consent from the adults and/or children concerned. Children have their own data protection rights. We assess parental requests against the child's understanding, the parent's authority and the child's best interests, and provide age-appropriate explanations.

We will store general student records for up to seven years after the end of the guardianship arrangement, unless we need to retain them for longer to comply with legal or safeguarding requirements.

Child Protection Records

April Well Limited is required to keep child protection records where there has been a safeguarding concern. There will be one file for each child and access is limited to the Director/DSL and other authorised people who need it for safeguarding or lawful case management. If it is necessary to share records (within our organisation or externally), we will ensure that they are kept confidential. We will use passwords and encryption when sharing electronic files. If the person responsible for managing our child protection records leaves, April Well Limited will appoint somebody to take over their role and arrange a proper handover.

We will store any child protection records until a child turns 25. Longer retention may be necessary for continuing safeguarding duties, legal claims or an applicable records category under our retention schedule; we review any continuing need before the scheduled deletion date.

Marketing

We will keep you up to date with our latest news and details about any services, upcoming events or training courses if you have told us that you are happy to receive marketing communications from us.

If you decide that you no longer want to hear from us, you can opt-out at any time. You can do this by contacting us using the details contained in this Policy, or by clicking on the 'unsubscribe' link contained in any email marketing communication you receive from us.

Links to third-party websites and services

This website may include links to other websites and applications that are operated by third parties. For example, we provide links to websites of other organisations, including accredited guardianship organisations and member schools. When you click on one of these links, you will be directed to that website.

We do not have any control over these third-party websites, and we cannot take any responsibility for any information you might give to them.

When you leave our website, we encourage you to read the privacy notice of every website you visit so you can understand how that website will collect and use your personal information.

Cookies

A cookie is a small file of letters and numbers which is downloaded to your device when you access a website. Websites may store or access cookies on your device; consent is required unless a PECR exception applies.

Cookies are used by many websites and have several different uses. For example, they can remember your preferences and count the number of people who have visited a website.

At April Well Limited, we use 'session cookies' and 'persistent cookies'.

'Session cookies' are those which expire at the end of your browser session. They allow a website to recognise and link the actions of a user during a browsing session. This means we can gather statistics to help us understand how our website is being used, and to improve its structure.

'Persistent cookies' are stored on a user's device in-between browsing sessions. They help us to recognise you as a unique visitor to our website and allow us to tailor the content of certain areas.

You can use your web browser to accept, decline, or delete cookies. You can also clear cookies at the end of your browsing session. Most web browsers automatically accept cookies, but you can modify your browser settings to decline cookies if you prefer. This may, however, prevent you from taking full advantage of our website. Browser settings do not replace consent where required. Non-exempt cookies require prior, informed consent and an equally easy way to withdraw it. A statistical-use exception applies only where all its legal conditions, including clear information and a simple objection mechanism, are met; advertising is not covered by that exception.

Your legal rights

We want to ensure that you are always in control of your personal information.

We have outlined below what your legal rights are in relation to your personal information, together with details as to how you can exercise them.

- **The right to access your personal information**

  You have the right to request a copy of the personal information we hold about you.

- **The right to edit and update your personal information**

  You have the right to request that your personal information is rectified if it is inaccurate or incomplete.

- **The right to request to have your personal information erased (also known as the 'right to be forgotten')**

  You have the right to request that your personal information is erased. However, this is not an absolute right, and it only applies in certain circumstances. For example, the law may require us to keep some types of personal information for a specific period of time.

  We will review each request on a case-by-case basis.

- **The right to restrict the processing of your personal information**

You have the right to request the restriction or suppression of your personal information. However, this is not an absolute right, and it only applies in certain circumstances.

When processing is restricted, we will continue to store your personal information, but will only use it where a legal exception permits, such as legal claims or protecting another person's rights.

- **The right to object to your personal information being used**

  You have the right to object to the processing of your personal information at any time. However, this is not an absolute right, and it only applies in certain circumstances.

  You do, however, have an absolute right to stop your personal information being used for direct marketing purposes.

- **The right to data portability**

  You have the right to request that we transfer your personal information from one organisation to another or give it to you. This applies to information you have provided, processed by automated means on consent or contract grounds; where applicable, it is supplied in a structured, commonly used, machine-readable format.

- **The right to complain to a supervisory authority if you believe we have not handled your personal information in accordance with data protection laws**

  You can make a complaint or raise a concern about how we process your personal information by contacting us using the details set out below. You may complain verbally or in writing to Xiaoying Chi using the contact details below. We acknowledge promptly under our Complaints Policy, and in all cases within 30 calendar days, investigate and keep you informed, and provide the outcome without undue delay. This does not extend rights-request deadlines.

  If you are not happy with how we have handled your complaint, or you believe that your data protection or privacy rights have been infringed, you have the right to complain to the Information Commissioner's Office (ICO). The ICO is the UK's independent body established to uphold information rights. Details: https://ico.org.uk/make-a-complaint/. Our internal process does not remove your right to complain to the ICO or seek a judicial remedy.

If you wish to exercise any of the rights outlined in this section, you may contact us verbally or in writing using the contact details below:

April Well Limited
Unit 39c, St Olavs Court Business Center
Lower Road
London

SE16 2XB
United Kingdom

Or send us an email: info@aprilwell.co.uk

We will endeavour to respond to all requests without delay, and in any event within one month of receiving your request. Where legally permitted for complexity or multiple requests, we may extend by up to two further months and explain why within the initial month. Any lawful pause for reasonably required clarification or identity checks will be explained.

Before responding to a request, we may be required to ask for further information and/or proof of your identity.

Please keep in mind that there are exceptions to the rights outlined above and although we will always try to respond to your satisfaction, there may be situations where we are unable to do so.

Changes to our Privacy Policy

This Privacy Policy will be regularly reviewed and may change from time to time. If it does, the most current version will always be available on this website.

We will keep our privacy notice under regular review. Our privacy notice will be reviewed annually or sooner if data protection legislation changes in the interim, therefore the review date will be 21 October 2027

This policy was last reviewed on: 21/10/2026

Signed: 

Name: Xiaoying Chi

Role: Director and Designated Safeguarding Lead (DSL)

Date: 21/10/2026