Data Protection Policy

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

Document Control

Title: Data Protection Policy

Owner: Xiaoying Chi, Director / DSL

Approved by: Xiaoying Chi

Document ID: AWP-DPP-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 at least annually in October and whenever statutory guidance or AEGIS Standards change. This revision reflects the AEGIS Quality Standards, September 2026, including Standards 2.7.1–2.7.6.

Table of Contents

Introduction and purpose 1
Scope 1
Definitions 1
Roles and responsibilities 2
Data protection principles 2
Keeping personal information secure 5
Managing personal data breaches 6
Responding to requests from individuals ('rights of data subjects') 7
Document retention 8
Data protection by design and default 8
Data processors 9
Record of processing activities 9
Data Protection Impact Assessments (DPIAs) 10
Appointment of a Data Protection Officer 10
AEGIS 11
Policy review 11

Introduction and purpose

This policy outlines our approach to handling personal information in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended, including by the Data (Use and Access) Act 2025.

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

Scope

This policy applies to the processing of personal information held by April Well Limited. This includes personal information about employees, volunteers, parents, students, visitors and any other individuals who engage with us. April Well Limited does not provide routine or long-term homestay accommodation. However, April Well may arrange or coordinate short-term emergency accommodation in clearly defined emergency or exceptional situations, in accordance with its Emergency Procedure and safeguarding policies. This policy applies to personal information processed in connection with any host family, emergency accommodation adult or external provider used or approved by April Well Limited.

This policy should be read in conjunction with the April Well Limited Privacy Policy. Our privacy notice must be publicly available, including on our website, and explain our purposes, lawful bases, disclosures, overseas transfers, retention, rights and contact details in accessible language, suitable for children where relevant.

Definitions

The following terms are used throughout this policy and it is important that you understand what they mean:

- **Personal data**: Any information relating to a person who can be identified, directly or indirectly, by reference to an identifier such as a name, an 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 person.
- **Data subject**: the identified or identifiable living individual to whom personal data relates
- **Controller**: A person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **Processor:** A person or organisation which processes personal data on behalf of the controller, and in accordance with their instructions.
- **Processing:** This is anything that you do with data, including collecting, recording, storing, using, analysing, combining, disclosing, or deleting it.
- **Special category data:** This is personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also includes genetic data, biometric data used to uniquely identify a person, and data concerning a person's health, their sex life, and sexual orientation.

Roles and responsibilities

April Well Limited is the data controller and is responsible for complying with the UK GDPR.

Director / Designated Safeguarding Lead (DSL)
— The Director / DSL has day-to-day responsibility for ensuring that this policy is implemented, adopted and adhered to by employees and any other individuals who process personal information on behalf of April Well Limited.

Employees and associates
— All employees and any other individuals who process personal information on behalf of April Well Limited are responsible for complying with this policy in its entirety. Failure to comply with this policy may result in disciplinary action being taken or the termination of an employment contract or agreement.

Data protection principles

The UK GDPR sets out several key principles which govern how April Well Limited handles personal information. Complying with these principles helps us to ensure that we comply with the law, and that our practices in relation to data protection are good.

The principles state that personal information must be:

- Processed in a way that is lawful, fair, and transparent *("lawfulness, fairness, and transparency")*
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes *("purpose limitation")*
- Adequate, relevant, and limited to what is necessary *("data minimisation")*
- Accurate, and where necessary, kept up to date *("accuracy")*

- Kept for no longer than is necessary *("storage limitation")*
- Processed in a way that ensures it is safe and secure, by means of appropriate technical and organisational measures *("integrity and confidentiality")*

The UK GDPR requires us to be able to evidence that we are complying with these principles. This is called the "accountability principle".

Lawfulness, fairness, and transparency

We only process personal information where there is a lawful basis for doing so. The lawful bases are as follows:

- Where the data subject has given us their consent to the processing
- Where processing is necessary for the performance of a contract, or to enter into a contract, with the data subject
- Where processing is necessary to comply with a legal obligation that we are subject to
- Where processing is necessary to protect the vital interests of the data subject or another person
- Where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, where the task or authority has a basis in UK law
- Where processing is necessary for the purposes of the legitimate interests pursued by April Well Limited or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

We will only process special category data where an Article 6 lawful basis and an applicable Article 9 condition have been identified. We document the condition and any required DPA 2018 Schedule 1 condition before processing, with an appropriate policy document where required. Relevant Article 9 conditions include:

- The data subject has given us their explicit consent
- The processing is necessary for the purposes of exercising or performing any right or obligation which is imposed on April Well Limited in relation to employment, social security, and social protection law
- The processing is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving consent
- The processing is necessary for the establishment, exercise, or defence of legal claims
- The processing is necessary for reasons of substantial public interest
- The processing is necessary for the assessment of the working capacity of an employee, subject to the applicable legal basis and professional confidentiality requirements

The principle of fairness means that personal information should be used in a way that the data subject would reasonably expect.

The UK GDPR defines 'consent' as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

When we rely on consent as the basis for processing personal information, we will ensure that the data subject is able to withdraw their consent as easily as they gave it, and at any time.

We will always use the most appropriate basis for processing personal information. Recognised legitimate interest under Article 6(1)(ea) may also apply where processing is necessary for a listed purpose, such as safeguarding children, and its specific conditions are met. We document our choice; for ordinary legitimate interests under Article 6(1)(f), we assess necessity and balance our interests against the individual's rights. Criminal offence data, including DBS information, additionally requires Article 10 authority or a DPA 2018 Schedule 1 condition, with an appropriate policy document where required.

The principle of transparency requires us to ensure that any information provided by us to data subjects about how their personal information will be processed, is concise, easily accessible, easy to understand, and written in plain language. We share relevant information with schools, parents, statutory services and other bodies only where necessary and lawful, recording the purpose, basis, recipient and decision. Consent is not always required for safeguarding, and seeking it must not delay protection or increase risk. Before using students' photographs in publicity or on our website, we obtain the necessary consent and apply suitable safeguards.

Purpose limitation

We will be clear from the very beginning as to why we are collecting personal information and what we intend to do with it.

We will only collect personal information for specified, explicit, and legitimate purposes, and we will not process information in any way that is incompatible with those purposes.

If things change, and we intend to use personal information for a different purpose, we will make sure that the new use is fair, lawful, and transparent. We will always inform data subjects before we use their personal information for a new purpose, and where the lawful basis relied upon for the original purpose was consent, we will obtain such consent again.

Data minimisation

The personal information that April Well Limited collects and processes will be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.

Accuracy

The personal information that April Well Limited collects and processes will be accurate and, where necessary, kept up to date, and will be corrected or deleted without delay when we are notified that the information is inaccurate.

All employees are required to update all relevant records if they become aware that any personal information is inaccurate.

Storage limitation

We do not keep personal information for longer than we need it.

We carefully consider how long we keep personal information for, and we justify our reasons for keeping it. Most of our retention periods are determined by legal timescales. For example, personal information relating to income tax contributions.

We have a retention schedule in place which details the types of personal information we hold, the reasons for holding it, and the retention period. This schedule forms part of our Record of processing activities **(see 'Record of processing activities')**.

We regularly review the data we hold and delete or securely destroy it when we no longer need it.

Integrity and confidentiality

We take our responsibilities under data protection laws very seriously and we will always ensure that we have appropriate security measures in place to protect the personal information we hold.

This means that we will have appropriate measures in place to protect personal information against unauthorised or unlawful processing, accidental loss, destruction, or damage.

April Well Limited employees are responsible for ensuring the security of the personal information processed by them in the performance of their duties and tasks.

Keeping personal information secure

We have appropriate technical and organisational measures in place to ensure that we process personal information securely, and to prevent personal information we hold being accidentally or deliberately compromised.

Technical measures

- We enforce strong password policies; passwords are changed at appropriate intervals and are not shared or used by others
- We ensure that laptops, USB/memory sticks and other portable devices containing personal information are encrypted
- We have a firewall, anti-virus, and anti-malware software in place
- We restrict access to systems, so personal information is only accessible to those people who need to use it as part of their work
- Personal information held electronically is backed up on each weekday, using AES-256 encryption

- Paper documents containing personal information are securely destroyed using a shredder when they are no longer required

Organisational measures

- We provide data protection awareness training to all employees during their induction and annually thereafter
- We have appropriate policies and procedures in place to ensure our employees fully understand their responsibilities under data protection laws
- We ensure that our employees and any other individuals who process personal information on behalf of April Well Limited, are aware of their individual responsibilities under data protection laws and how these apply to their areas of work
- We promptly investigate all suspected personal data breaches; we always make the appropriate external notifications (where applicable) and seek to learn any lessons from the incident to reduce the risk of reoccurrence.
- Paper documents containing personal information are securely locked away when not in use
- Paper documents containing personal information are securely destroyed using shredders when they are no longer needed
- Employees take every opportunity to ensure that the personal information we hold is accurate and kept up to date
- Employees do not disclose personal information to any unauthorised persons, both externally and within April Well Limited

We regularly test, assess, and evaluate the effectiveness of the measures we have put in place, and act on the results of those tests where they highlight areas for improvement.

Managing personal data breaches

We have a procedure in place for managing and responding to personal data breaches.

A 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.

Examples of personal data breaches include:

- Sending personal data to the wrong person
- Access to personal data by an unauthorised third party
- Devices or equipment containing personal data being lost or stolen

All suspected personal data breaches and security incidents must be reported without delay to the **Director / DSL**. All personal data breaches will be investigated promptly and recorded on our internal data breach register. Records include the facts, effects, remedial action and reasons for notification decisions, including decisions not to notify.

The **Director / DSL** is responsible for deciding whether a personal data breach needs to be reported to the ICO and any affected data subjects, and for agreeing any external notifications. Absence must not delay containment, risk assessment or statutory notification. Staff should seek urgent ICO advice if the Director / DSL cannot be reached; safeguarding concerns also follow our Safeguarding and Child Protection Policy immediately.

We notify the ICO unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Where notification is required, April Well Limited will report it without undue delay and, where feasible, within 72 hours of becoming aware of it. Where the notification is made after 72 hours, the reasons must be given to the ICO and recorded. Missing details may follow in phases without undue further delay; we must not wait for a completed investigation.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject(s), the **Director / DSL** will communicate the personal data breach to the data subject(s) without undue delay.

When informing the data subject(s) about the breach, we will provide in clear, plain language, the following information:

- Details about the nature of the breach
- The name and contact details of the organisational point of contact, who the data subject(s) can contact if they require further information
- The likely consequences of the breach
- Measures taken, or proposed to be taken, to address the breach including measures to mitigate possible adverse effects

Responding to requests from individuals ('rights of data subjects')

The UK GDPR provides data subjects with a number of rights in relation to their personal information.

These are:

- The right to request a copy of the personal information we hold about them
- The right to request that inaccurate or incomplete information about them is rectified
- The right to request that their personal information is deleted
- The right to request that the processing of their personal information is restricted
- The right to data portability
- The right to object to the processing of their information
- The right to complain to the ICO if they are not happy with how their personal information has been processed, or they feel their data protection rights have been infringed

We respond to rights requests without undue delay and within one calendar month of receipt, subject to permitted extensions and adjustments below. Where necessary because of complexity or the number of requests from the same individual, we may extend by up to two further months, explaining the reasons within the first month. Requests may be made verbally or in writing to any staff member; no special form is required. Forward them promptly to the Director / DSL at info@aprilwell.co.uk.

Any identity or representative-authority checks must be necessary and proportionate and requested promptly. For subject access requests, the response period starts when reasonably required identity or authority evidence is received. If clarification is reasonably required, the clock pauses on the day we ask and resumes the day after clarification arrives; we cannot force the person to narrow their request. If they repeat their request, we make reasonable and proportionate searches. Supplementary information reasonably available without clarification remains due within one month. Children's rights belong to the child: assess competence and best interests before accepting a parent's or representative's request, and verify their authority.

There may be exceptions to the rights outlined above; each request we receive will be reviewed on a case-by-case basis. Any refusal must be justified and explained within the applicable deadline, including the rights to complain to us and the ICO and seek a judicial remedy. Data protection complaints may be made verbally or in writing using the contact details on the cover. We acknowledge promptly under our Complaints Policy and in all cases within 30 calendar days, investigate and provide progress updates and the outcome without undue delay, and record actions taken. Our internal process does not remove the right to complain to the ICO at https://ico.org.uk/make-a-complaint/ or extend rights-request or breach-reporting deadlines.

Document retention

We do not keep personal information for longer than we need it.

We carefully consider how long we keep personal information for, and we justify our reasons for keeping it. Most of our retention periods are determined by legal timescales. For example, personal information relating to income tax contributions.

We have a retention schedule in place which details the types of personal information we hold, the reasons for holding it, and the retention period. This schedule forms part of our Record of processing activities **(see 'Record of processing activities')**.

We regularly review the data we hold and delete or securely destroy it when we no longer need it.

Data protection by design and default

We consider data protection and privacy issues upfront in everything we do. We are required to do this under the UK GDPR.

We make sure that when we are designing and implementing a new organisational system, service, or practice, we consider the data protection issues before we begin. We also make sure, by default, that we only process personal information where it is necessary to do so.

Data processors

Whenever we use a third party to process personal information on our behalf, we will always undertake appropriate due diligence and ensure a data processing agreement is in place. The agreement must meet the applicable requirements of UK GDPR Article 28.

We only use processors that provide us with sufficient guarantees about their security measures. Before any restricted transfer outside the UK, including overseas access, we establish a lawful transfer route: UK adequacy regulations, appropriate safeguards with the required data protection test, or an applicable Article 49 exception. We record the route and any additional protections.

Record of processing activities

April Well Limited maintains a record of its processing activities, as is required under Article 30 of the UK GDPR.

This record is held in electronic format and contains the following information:

- Our organisation name and contact details
- A description of the personal information we process
- Categories of data subjects
- Purposes of the processing
- Recipients of the personal information
- The name of any countries or organisations outside the UK that we transfer personal information to, together with information about the safeguards in place
- Retention periods
- A general description of our technical and organisational security measures e.g. encryption, access controls, and training.

We regularly review the personal information we process and update this record accordingly.

This record will be made available to the ICO, if requested.

Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process that helps us to identify and minimise the data protection risks associated with a project, process, or activity involving the processing of personal information.

We are required to carry out a DPIA for any processing that is likely to result in a high risk to individuals. We will also carry out a DPIA for any other major project which requires the processing of personal information, because it is good practice to do so.

The DPIA will:

- Describe the nature, scope, context, and purposes of processing
- Assess necessity, proportionality, and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks

We will record the outcome of the DPIA and implement the measures identified. The assessment must precede the processing. If high residual risk cannot be reduced, we consult the ICO before starting that processing.

Appointment of a Data Protection Officer

Under Article 37 of the UK GDPR, controllers and processors are required to appoint a Data Protection Officer if:

- The processing is carried out by a public authority or body
- The core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of individuals on a large scale
- The core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences

The status of our organisation and the scope of our processing activities means that we are not required to appoint a Data Protection Officer.

We will document this assessment and keep the decision under review, should our processing activities change.

AEGIS

As part of the AEGIS Gold Standard accreditation process, April Well Limited may be required to provide AEGIS with relevant records, such as contact details for partner schools, names of students included in the inspection sample, safeguarding records, emergency accommodation records, transport records, staff records, and records relating to any host family, emergency accommodation adult or external provider used or approved by April Well Limited. We secure and record permission from the individuals concerned before supplying their contact details to AEGIS, as required by Standard 2.7.6, and explain inspection sharing in our privacy notice. Other records are disclosed only where necessary and lawful, with additional safeguards for sensitive information. Inspection contact lists and working copies are deleted when no longer needed for the inspection, in line with AEGIS requirements; original company records remain subject to our retention schedule and any safeguarding or legal retention duties.

Policy review

We are committed to reviewing our policy and good practice annually.

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

Signed: 

Name: Xiaoying Chi

Role: Director and Designated Safeguarding Lead (DSL)

Date: 21/10/2026