Kids 4 kids
童協基金會

DATA PROTECTION POLICY

Kids4Kids Limited

Version 3.0

(August 2025)

Table of Contents

1. OVERVIEW

This Data Privacy Policy (the "**Policy**") and corresponding policy documents apply to all services provided by Kids4Kids Limited, a company limited by guarantee incorporated in Hong Kong (the "**Company**"). It sets out how the Company may collect, use, disclose and protect personal information.

In its everyday operations the Company makes use of a variety of data about identifiable individuals, including data about:

- Its current, past and prospective employees
- Recipients or prospective recipients of its services
- Users of its websites
- Its members, donors, volunteers or prospective members, donors and volunteers
- Other stakeholders

In collecting and using this data, the Company is subject to a variety of laws and regulations, including but not limited to the Personal Data (Privacy) Ordinance (PDPO) (the "**PDPO**" or "**Rules**"), which control how such activities may be carried out and the safeguards that must be put in place to protect the data.

The purpose of this Policy is to describe the steps the Company is taking to ensure that it complies with these Rules and to safeguard the privacy rights of individuals.

This Policy applies to all systems, people and processes that constitute the Company's information systems, including members, directors, employees, suppliers and other third parties who have access to the Company's systems.

2. DEFINITIONS

The most fundamental definitions with respect to this Policy are as follows:

personal data	*any data—* *(a)relating directly or indirectly to a living individual;* *(b)from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and* *(c)in a form in which access to or processing of the data is practicable*
processing	*in relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise*
data user	*in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data*
data subject	*in relation to personal data, means the individual who is the subject of the data*

PCPD	*the Office of the Privacy Commissioner for Personal Data, Hong Kong*
PDPO	*Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong)*

3. FUNDAMENTAL PRINCIPLES OF DATA PRIVACY LAWS

There are a number of fundamental principles upon which data privacy laws are based. These are as follows:

lawfulness, fairness and transparency	*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.*
collection purpose and means	*Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.* *All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.* *Data collected should be necessary but not excessive.*
accuracy and retention	*Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.*
use	*Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.*
storage limitation	*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest (including historical interest) or where the erasure of personal data is prohibited by law.*

integrity and confidentiality	*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*
openness	*All practicable steps shall be taken to ensure openness of the data users' personal data policies and practices, the kind of personal data held and the main purposes for holding it.*
data access and correction	*A data subject must be given access to his personal data and make corrections where the data is inaccurate.*
accountability	*The data user shall be responsible for, and be able to demonstrate compliance with all of the above.*

The Company will ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of any new methods of processing.

4. RIGHTS OF THE DATA SUBJECT

Data subjects typically also have the following rights under the applicable Rules:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the "right to be forgotten")
- The right to restrict processing
- The right to data portability
- The right to object
- Rights not to be subject to automated decision making and profiling.

Each of these rights is supported by the Company's appropriate procedures that ensure required action within the timescales outlined in Table 1 below.

5. PROCESSING DATA

In Hong Kong, the primary lawful basis for the Company to process personal data is to obtain explicit, informed consent from the data subject. Other lawful bases may apply depending on the specific circumstances. The Company will seek legal advice when uncertain.

5.1 Consent

Unless otherwise allowed under the Rules, the Company will ***always*** obtain explicit, voluntary, and informed consent from data subjects for data collection and processing for directly related or new purposes. For children's personal data, parental or guardian consent will always be obtained.

Transparent information about the Company's use of personal data will be provided to data subjects at the time that consent is obtained, including explanations of:

- The purposes for which personal data will be used following collection;
- The types of data collected;
- Whether it is obligatory or voluntary for the individual to supply his or her personal data, and where it is obligatory, the consequences of failure to supply such personal data;
- The Classes of possible transferees to whom personal data collected may be transferred or disclosed;The rights of the data subject, including the right to access, correct and withdraw consent at any time;
- The name (or job title) and contact details of the person responsible for handling any data access and data correction requests.

This information will be provided in an accessible form, written in clear language and free of charge. This is called the "Personal Information Collection Statement".

If personal data is not obtained directly from the data subject, the Company will provide this information to the data subject within a reasonable period after the data is obtained, and no later than one month.

5.2 Performance of a Contract

Where the personal data collected and processed is required to fulfil a contract with the data subject, explicit consent is not required (e.g. delivery requires an address).

5.3 Legal Obligation

If required by law or regulation, data may be processed without explicit consent (e.g. tax filings, mandatory public sector reporting).

5.4 Vital Interests of the Data Subject

Where processing of personal data is necessary to protect the vital interests of the data subject or of another natural person, this may serve as the lawful basis for processing (e.g. emergency medical information).

The Company will retain documented evidence to demonstrate that this basis applies.

5.5 Task Carried Out in the Public Interest

The Company may process personal data without obtaining consent when performing a task that it believes is in the public interest or as part of an official duty.

The assessment of whether the task is in the public interest or constitutes an official duty will be documented and made available as evidence, if required.

5.6 Legitimate Interests

Processing of specific personal data may be based on the Company's legitimate interests, provided that such processing does not unduly infringe the rights and freedoms of the data subject.

The reasoning behind this view will be documented and may include examples such as:

- Processing employee data for internal analytics or performance monitoring;
- Ensuring the security of the Company's IT systems.

6. PRIVACY BY DESIGN

The Company has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data is subject to thorough consideration of privacy issues. This includes the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be collected, stored, processed, and for what purposes;
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to achieve the stated purpose(s);
- Identification and assessment of risks to individuals resulting from the processing personal data;
- Implementation of technical and organization controls to address the identified risks and to demonstrate compliance with the applicable rules and principles.

The Company will also consider implementing techniques such as:

- Data minimization (e.g., collecting only data that is strictly necessary);
- Pseudonymization (e.g., replacing identifiers with pseudonyms to reduce identification risks);
- Encryption (e.g., securing data to prevent unauthorized access).

The Privacy by Design principle will apply to all stages of system design and development, ensuring that data protection is a core consideration from the outset.

7. CONTRACTS COVERING THE PROCESSING OF PERSONAL DATA

The Company will ensure that all relationships involving the processing of personal data are governed by documented contracts that include the specific information and terms required by applicable rules.

These contracts will include, at a minimum,

- The purpose for which the personal data is entrusted to the data processor;
- Data retention requirements, including timelines for deletion or return of data when processing ends;
- Provisions to prevent unauthorized or accidental access, processing, erasure, loss, or use of personal data;
- A requirement for the data processor to implement appropriate technical and organizational measures to ensure data security and compliance with the PDPO;
- A prohibition against the data processor using the data for purposes other than those specified in the contract.

Where appropriate, the Company will conduct due diligence on data processors to ensure they have adequate safeguards in place for personal data protection.

All such contracts should be reviewed by the Executive Director and the Company's pro bono lawyers.

8. INTERNATIONAL TRANSFERS OF PERSONAL DATA

Each transfer of personal data to a location outside Hong Kong will be carefully reviewed prior to the transfer takes place to ensure compliance with the Rules.

This assessment will include:

- Determining whether the receiving country has adequate safeguards for personal data protection;
- Ensuring that appropriate measures, such as contractual safeguards, are in place to protect the transferred data;
- Regularly monitoring changes in data protection laws and practices in the receiving country.

Where the collection, holding, processing or use of personal data:

(a) takes place in Hong Kong; or

(b) is controlled by any member of the Company or a data user whose principal place of business is in Hong Kong,

the Company will comply with the "Guidance Note on Cross Border Transfer of Personal Data (Dec 2014)" published by the PDPC.[1]

[1] https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf

Under this guidance:

1. Personal data may not be transferred to a place outside Hong Kong unless one of the following applies:
   - The data subject has provided written consent to the transfer; or
   - Other circumstances permitted by Section 33(2) of the PDPO apply. *(Note: Section 33 has not yet come into effect but remains an important consideration.)*

Where feasible, the Company will use contracts containing the "Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data (May 2022)" issued by the PDPC.[2] These clauses provide clear safeguards for both data users and processors involved in international transfers.

Currently the Company does not transfer any personal data outside Hong Kong and any such transfer must obtain prior written consent from the Executive Director.

9. PERSONAL DATA FOR DIRECT MARKETING PURPOSES

Before the use of personal data, or provision of personal data to third parties, for direct marketing purposes, data subject must be explicitly informed of the following in a manner that is easily understandable and readable:

1. The Company's intention to use their personal data or provide their personal data to third parties for direct marketing and that the data will only be used or transferred with data subject's explicit consent;
2. The types of personal data that will be used for direct marketing;
3. The specific classes of marketing subjects[3] (to a reasonable degree of certainty) to which the proposed direct marketing will relate;
4. In the case of provision of personal data to third parties, the classes of third parties (in reasonably specific terms) to whom the data subject's personal data will be provided, and whether the transfer is for gain;
5. the data subject's right to require the Company to stop using their personal data for direct marketing purposes.

The data subject must be provided with a means to communicate their consent (or an indication of no objection) to the proposed direct marketing without charge.

To qualify as an indication of no objection, the data subject concerned must have explicitly indicated that he/she did not object to the use and/or provision of his/her personal data to another for use in direct marketing. Hence, consent cannot be inferred from the data subject's non-response. In other words, silence does not constitute consent.

[2] https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_model_contractual_clauses.pdf
[3] "Marketing subjects" means the goods, services or facilities being marketed or the purpose for which any donation or contribution is requested.

Further, data subjects should not be asked to give a "bundled consent" agreeing to the general terms and conditions for the provision of the services and the use of his personal data for direct marketing purposes. There should be an additional checkbox for the data subject to consent to the purpose of direct marketing.

Where consent is sought for the provision of personal data to a third party for direct marketing purposes:

- The consent must be in writing.
- If consent is given orally, it must be followed by a written confirmation within 14 days. The confirmation must confirm:
    - The date of receipt of oral consent;
    - The types of personal data to be used;
    - The classes of marketing subjects.

Reasonable time (approximately 14 days) should be allowed for the data subject to dispute the written confirmation before the Company begins using the personal data in direct marketing.

On the first time that data subject's personal data is used in direct marketing, the data subject should be informed that they may, at any time, require the Company to cease using their personal data in direct marketing without charge, irrespective of whether the personal data was collected directly from the data subject or from other sources. The Company must comply with such requests promptly.

The Company will maintain and regularly update the record of consents and opt-out list to ensure compliance with the PDPO.

10. PERSONAL DATA FOR RECRUITMENT AND EMPLOYMENT PURPOSES

Data collection from prospective employees

The Company may invite a job applicant to fill out an online data collection form or subject information by email. Such practice amounts to the collection of personal data and the relevant staff must take all practical steps to ensure that job applicants are explicitly informed, on or before collection, of the followings:

(i) it is obligatory or voluntary for them to supply the data; and

(ii) where it is obligatory for them to supply the data, the consequences for them if they fail to supply the data. For instance, their application would not be further processed if they fail to provide educational proof or professional accreditation certificate that is necessary to discharge the job duties required from that particular role; and

(iii) the purpose (in general or specific terms) for which the data is to be used; and

(iv) the classes of persons to whom the data may be transferred.

On or before the data is used for the purpose for which it is collected, the prospective employee must be notified of the following:

(i) their rights to request access to and correction of their personal data; and
(ii) the name or job title, and contact details of the individual who is to handle any such requests (e.g. the Company's Data Protection Officer).

The Company will take all practical steps to maintain the confidentiality of personal data of job applicants during its collection, processing and storage. Staff authorised to access personal data must demonstrate integrity, prudence and competence and be well-versed with the Company's privacy policy and practices.

The staff responsible for collection of personal data of prospective employees must notify the data subjects the purpose of collection and other relevant information by presenting to a Personal Information Collection Statement ("**PICS**") in the form and substance set out in *Code of Practice on Human Resource Management: Compliance Guide for Employers and Human Resource Management Practitioners ("**Code**")* issued by the PCPD or other guidance material that may be issued by PCPD from time to time. The completed PICS must be retained for internal record.

The Company may, no earlier at the time of making a conditional offer of employment to a selected candidate, collect personal data concerning the health condition of the candidate by means of a pre-employment medical examination, provided that:

(i) the personal data directly relates to the inherent requirements of the job;
(ii) the employment is conditional upon the fulfilment of the medical examination; and
(iii) the personal data is collected by means that are fair in the circumstances and are not excessive in relation to the purpose.

Data collection from current employees

The Company may retain personal data of the employee for the purpose of the employment collected during the recruitment process, and may collect supplementary personal data from the employee for the purposes of employment and other related human resource management functions, such as bank details for the purpose of payment of salary.

In the course of employment of the employee, the Company may further compile information about the employee, which may include the following:

(i) records of remuneration and benefits paid to the employee;
(ii) records of job postings, transfer and training;
(iii) records of medical checks, sick leave and other medical claims;
(iv) written records of disciplinary proceedings involving the employee;
(v) performance appraisal reports of the employee;

(vi) written reports of staff planning exercises involving the employee; and
(vii) written reports of promotion exercises involving the employee.

The Company shall take all practical steps to ensure that the employment-related data it holds about employees is accurate having regard to the purpose for which the data is used. Disclosure of employment-related data of employees to a third party is prohibited, unless prior express and voluntary consent is or such disclosure is required by law or by statutory authorities.

Retention of data of former employees

The Company may retain personal data pertaining to a former employee to fulfil its obligations to the former employee and its legal obligations under certain ordinance, which include the following:

(i) statutory requirements, such as retention of salaries' tax records, business records, sick leave records etc.;
(ii) administer any remaining duties in respect of former employees under MPF scheme;
(iii) defend the Company in any civil suit or criminal prosecution under ordinances, such as the Employees Compensation Ordinance.
(iv) re-employ a former employee if there is a reasonable likelihood of the individual re-applying for employment;
(v) provide job references at the request of the employee.

The Company shall retain the data of any departing employee for a period of no longer than seven (7) years calculated from the date of cessation of employment, unless there is a subsisting reason that obliges the Company to retain the data for a longer period. Generally speaking, actual or potential legal proceedings may constitute a subsisting reason for the Company to retain the relevant data for a longer period.

Express and voluntary consent must be obtained from the former employee before providing a job reference to a third party.

Retention of data of rejected applicants

The Company shall retain the data of any rejected applicant for a period of no longer than two (2) years calculated from the date the applicant is rejected unless the individual concerned has given express consent for the data to be retained for a longer period, or there is a subsisting reason that obliges the Company to retain the data for a longer period.

It is the Company's policy to include a statement in the recruitment advertisement about the data collection purposes and the Company's contact information.

11. DATA COLLECTION FROM CHILDREN

The Company shall take special care in collecting personal data from children. It is best practice to avoid directly collecting personal data from children if there is alternative way of achieving the purpose. For instance, the Company shall encourage the children's parents or teachers to be involved when collecting data from them.

The Company shall use clear, simple and age-appropriate language in the collection process and suggest children to consult their parents before providing their personal data. When collecting the data from children, the Company shall obtain consent to such collection from the parents or guardian of the children.

The Company may consider developing a single place on its website, such as a "dashboard" for each child that has provided personal data to find out what personal data has been collected or maintained through the Company's website. Such "dashboard" should only be accessible by that child. Where younger children are involved, the Company may extend access to the "dashboard" to their parents so that they can help the relevant child to manage their own personal data privacy.

Children may not be aware of their rights to have personal data corrected or removed. The Company should therefore ensure that children and their parents or teachers are well informed of their rights and offer them with an easy way to do so.

When children are allowed to use their social network accounts for interaction (such as logging in, using "like", "share" or similar action that may show the children's social network account names) with their online platforms, the Company should explain clearly to children the implications of using social network accounts.

As a best practice, when a website redirects children to another site, clear notice should be given to the children. This is particularly important when the redirected site is not under the direct control of the Company. In the absence of such notice, children run the risk of unintentionally or unknowingly disclosing their own personal data.

Even for non-profit making purposes, the promotion or advertising of services (including solicitation of donation) is considered as direct marketing activities. If a child's personal data is intended for use in direct marketing, the Company must inform the child and his parents accordingly, obtain their prior consent and provide them with a channel through which their consent may be communicated.

12. BREACH NOTIFICATION POLICY

A data breach is a suspected breach of data security of personal data held by a data user, which exposes the data to the risk of unauthorised or accidental access, processing, erasure, loss or use. It is the Company's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. The Company shall handle data breaches by following the steps set forth below:

(i) Immediately gather essential information of data breach to assess the impact on data subjects and to identify appropriate mitigation measures;
(ii) Take appropriate steps to contain the breach immediately and as effectively as possible and remedial steps to lessen the damage to the affected data subjects;
(iii) Assess the risk of harm after gathering all essential information, taking into account the kind, sensitivity and the amount of personal data involved, the circumstances leading to the data breach, the nature of harm, the duration of breach, etc.;
(iv) Consider giving data breach notification to the PCPD, the affected data subjects, and law enforcement agencies, the relevant regulators and other parties who may be able to take remedial actions as soon as practicable after becoming aware of the data breach; and
(v) Document the data breach incident for post-breach review.

For more details, please refer to the "Guidance on Data Breach Handling and Data Breach Notifications" published by the PCPD.[4]

13. GUIDELINES ON USE OF GENERATIVE AI TOOLS

Employees and contractors ("AI Users") may use generative artificial intelligence ("Gen AI") tools only if expressly approved by the Executive Director for work-related purposes. The use of Gen AI tools is intended to enhance productivity, creativity, and operational efficiency while ensuring strict compliance with all applicable laws.

The use of Gen AI tools must comply with the following conditions:
(i) Gen AI tools should be used only for tasks such as drafting, summarizing, content creation, translation, and administrative duties that align with your job responsibilities and the Company's needs.
(ii) Personal Data and Confidentiality:
- Do not input any personal data or confidential information, including that of colleagues or third parties, into Gen AI tools without prior written approval and safeguards.
- Assume that information entered into public AI tools may be retained or accessed by others.
- Avoid sharing sensitive data such as passwords, health information, personnel details, or any private data.
- Always anonymize or generalize data before inputting it.
- Disable chat history or data retention features if available.
- Decline any AI platform requests for device access permissions.

(iii) Use of Gen AI tools must comply with the PDPO and this Policy. Report any suspected data security or privacy breaches related to AI use immediately to your supervisor, who will escalate the matter to the relevant department.
(iv) AI-generated outputs may contain errors, inaccuracies, or biases. Always review and verify AI-generated content before using it in your work.

[4] https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf

(v) Security and Access Controls:
- Use only Company-provided IT devices to access Gen AI tools.
- Access is limited to authorized and trained employees.
- Avoid using untrusted or public networks when accessing these tools.
- Use your Company email for AI tool registrations and communications.

(vi) Report any suspected misuse, data breach, or abnormal AI-generated content promptly as per the Company's incident response procedures set out in [Section 12] of this Policy.

(vii) Do not use Gen AI tools for unlawful, harmful, or discriminatory purposes. Report any biased or inappropriate AI outputs immediately.

(viii) Non-compliance with these guidelines may lead to disciplinary action, including termination, and potential legal consequences.

For more details, please refer to the "Checklist on Guidelines for the Use of Generative AI by Employees" published by the PCPD.[5]

Please also note that there is a risk of losing the intellectual property ownership rights in works created by Gen AI tools. All staff should therefore obtain the prior approval of the Company before using Gen AI tools to create works on behalf of the Company.

14. ADDRESSING COMPLIANCE WITH DATA PRIVACY RULES

The following actions are undertaken to ensure that the Company complies at all times with the accountability principle of the Rules:

(i) The legal basis for processing personal data is clear and unambiguous.

(ii) The Company's personal data policies and practices regarding the types of personal data it holds and how the data is used should be made known to the public.

(iii) Before and at the time of collection of personal data, all data subjects must be informed of (i) the purposes for which the personal data is to be used; (ii) the classes of persons to whom the data may be transferred; (iii) whether it is obligatory or voluntary to supply their personal data and, where it is obligatory, the consequences of failure to supply their personal data; (iv) the intention to use personal data for direct marketing (if applicable); (v) the right of data subject to request access to and correction of his/her personal data; and (vi) the name or job title, and address of the individuals to whom access and correction requests may be made. The above information must be easy to read and understand.

(iv) All staff involved in handling personal data understand their responsibilities for following good data protection practice.

(v) Training in data protection will be provided to all staff annually.

(vi) Rules regarding consent are followed.

[5] https://www.pcpd.org.hk/english/resources_centre/publications/files/guidelines_ai_employees.pdf

(vii) Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively.
(viii) Regular reviews of procedures involving personal data are carried out.
(ix) Privacy by design is adopted for all new or changed systems and processes.
(x) The following documentation of processing activities is recorded:

- Organisation name and relevant details
- Purpose of the personal data processing
- Categories of individuals and personal data processed
- Categories of personal data recipients
- Agreements and mechanisms for transfers of personal data to other countries including details of controls in place
- Personal data retention schedules
- List of data subjects who have given, not given or withdrawn their consent
- Logbook of refusals of data subjects' access to personal data or request for data correction
- Relevant technical and organisational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with data protection.

TABLE 1

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access *(Note 1)*	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights not to be subject to automated decision making and profiling.	As soon as reasonably practicable
Rights to stop using personal data for direct marketing purposes	Without undue delay

Note:

1. If the Company does not hold the requested data or refuses to comply with such request, the Company is required to inform the requestor in writing within one month.