Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

bestchance is the operating name of bestchance Child Family Care

Privacy and Records Management Policy

Objective

bestchance (we, our, us) is working for the growth of individuals through mutual respect and responsibility, within a harmonious and supportive work environment.

We recognise the importance of protecting the privacy and the rights of individuals in relation to their personal information. This document is our privacy policy and it tells you how we collect and manage your personal information.

We respect your rights to privacy under the Privacy Act 1988 (Cth) (Act), the Health Records Act 2001, the information Privacy Act 2000 and we comply with their requirements in respect of the collection, management and disclosure of your personal information.

Definitions

Health information - any information or an opinion about the physical, mental or psychological health or ability (at any time) of an individual.

Health Records Act 2001 - Victorian legislation that regulates the management and privacy of health information handled by public and private sector bodies in Victoria.

Information Privacy Act 2000 - Victorian legislation that protects personal information held by Victorian Government agencies, statutory bodies, local councils and some organisations, such as **bestchance** contracted to provide a service or program for government.

Privacy Officer - the first point of contact for advice on privacy matters related to **bestchance.**

Personal information - recorded information, including images or opinion, whether true or not, about a living individual whose identity can reasonably be ascertained. This typically includes a person's name, address, contact details, date of birth, gender, sexual orientation and race.

Privacy breach - an act or practice that interferes with the privacy of an individual by being contrary to, or inconsistent with, one or more of the Information Privacy Principles (*refer attachment from the Office of the Australian Information Commissioner – Privacy Fact Sheet 17 – Australian Privacy Principles*).

Sensitive information - information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political party, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preference or practices, or criminal record. This is also considered to be personal information.

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

Unique identifier - a symbol or code, usually a number, assigned by an organisation to an individual to distinctively identify that individual while reducing privacy concerns by avoiding use of the person's name.

Scope

This policy applies to **bestchance** staff, students on placement, volunteers, parents/guardians, children and others attending the programs and activities of **bestchance.**

What is your personal information?

When used in this privacy policy, the term "personal information" has the meaning given to it in the Act. In general terms, it is any information that can be used to personally identify you. This may include your name, address, telephone number, email address and profession or occupation. If the information we collect personally identifies you, or you are reasonably identifiable from it, the information will be considered personal information.

What personal information do we collect and hold?

We may collect the following types of personal information:

- name;
- mailing or street address;
- email address;
- telephone number;
- facsimile number;
- age or birth date;
- profession, occupation or job title;
- gender, sexual orientation and race;
- details of the services you have purchased from us or which you have enquired about, together with any additional information necessary to deliver those products and services and to respond to your enquiries;
- any additional information relating to you that you provide to us directly through our websites or indirectly through use of our websites or online presence, through our representatives or otherwise;
- Photos and videos;
- health information including information or opinion about the physical or mental health, or disability, of an individual;
- an individual's expressed preferences about the future provision of child, kindergarten, health, disability services;
- the nature of child, kindergarten, health or disability services that have been, or are to be, provided to an individual;
- information originally collected in the course of providing a child, kindergarten, disability or health service to an individual;
- information you provide to us through our services, kindergartens, school, child care centres, family or early childhood intervention services or interactions with our representatives from time to time;

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

We may also collect some information that is not personal information because it does not identify you or anyone else. For example, we may collect anonymous answers to surveys or aggregated information about how users use our website.

How do we collect your personal information?

We collect your personal information directly from you unless it is unreasonable or impracticable to do so. When collecting personal information from you, we may collect in ways including:

- through your access and use of our website;
- during conversations between you and our representatives; or
- when you complete an enrolment, application, request for service or purchase order.

We may also collect personal information from third parties including:

- from third party companies such as credit reporting agencies, law enforcement agencies and other government entities

Gaining consent to collect and use personal information

Consent must be gained to collect, use and where appropriate/necessary, forward to a third party. A person's consent is sought unless there are sound, justifiable reasons permitted by the relevant legislation and privacy principles.

Criteria for consent:

(i). Consent must be informed
The person from whom the information is collected must be informed as to what they are consenting to. This means knowing –

- what is being collected, used or disclosed and why;
- who/what organisation is collecting, using or receiving/likely to receive the information; and
- the consequences, if any, if consent is not given.

(ii). Consent must be freely given
There must be no coercion in obtaining the person's consent. If a genuine choice is not offered, the proposed action can only proceed if permitted by legislation.

(iii). Consent must be specific
Consent is to be sought for the collection or use of specific information, for an identified purpose, by identified people/organisation, for an identified period of time.

(iv). Consent must be current
Consent must apply to a person's circumstances at the time; it should be able to be revoked at any time.

'Express' and 'Implied' Consent
There are two types of consent – 'express' and 'implied'.

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

- Express consent is unequivocal consent that does not require any inference.
- Implied consent is consent that can only be inferred by the actions of the person from whom the consent is sought.

Where possible/appropriate, express consent must be sought/obtained. Where a person's consent is sought or obtained verbally, detailed file notes should be kept regarding the name of the person giving consent, the date and time consent was given and whether consent was obtained over the phone or in person.
Where written consent is sought, the request must be easy to find and expressed in clear language.

Cookies

In some cases we may also collect your personal information through the use of cookies. When you access our website, we may send a "cookie" (which is a small summary file containing a unique ID number) to your computer. This enables us to recognise your computer and greet you each time you visit our website without bothering you with a request to register. It also enables us to keep track of products or services you view so that, if you consent, we can send you news about those products or services. We also use cookies to measure traffic patterns, to determine which areas of our website have been visited and to measure transaction patterns in the aggregate. We use this to research our users' habits so that we can improve our online products and services. Our cookies do not collect personal information. If you do not wish to receive cookies, you can set your browser so that your computer does not accept them.

We may log IP addresses (that is, the electronic addresses of computers connected to the internet) to analyse trends, administer the website, track users movements, and gather broad demographic information.

What happens if we can't collect your personal information?

If you do not provide us with the personal information described above, some or all of the following may happen:

- we may not be able to provide the requested services or products to you, either to the same standard or at all;
- we may not be able to provide you with information about services and products that you may want, including information about government funding, support or special promotions; or
- we may be unable to tailor the content of our websites to your preferences and your experience of our websites may not be as enjoyable or useful.

For what purposes do we collect, hold, use and disclose your personal information?

We collect personal information about you so that we can perform our business activities and functions and to provide best possible quality of customer service. We collect, hold, use and disclose your personal information for the following purposes:

• to provide services and products to you and to send communications requested by you;

• to answer enquiries and provide information or advice about existing and new products or services;

• to provide you with access to protected areas of our website;

• to assess the performance of the website and to improve the operation of the website;

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

• to conduct business processing functions including providing personal information to our related bodies corporate, contractors, service providers or other third parties;

• for the administrative, marketing (including direct marketing), planning, product or service development, quality control and research purposes of bestchance, its related bodies corporate, contractors or service providers;

• to provide your updated personal information to our related bodies corporate, contractors or service providers; • to update our records and keep your contact details up to date;

• to process and respond to any complaint made by you; and

• to comply with any law, rule, regulation, lawful and binding determination, decision or direction of a regulator, or in co-operation with any governmental authority of any country (or political sub-division of a country).

Your personal information will not be shared, sold, rented or disclosed other than as described in this Privacy Policy.

To whom may we disclose your information?

We may disclose your personal information to:

- our employees, related bodies corporate, contractors or service providers for the purposes of operation of our website or our business, fulfilling requests by you, and to otherwise provide products and services to you including, without limitation, web hosting providers, IT systems administrators, mailing houses, payment processors, data entry service providers, electronic network administrators, debt collectors, and professional advisors such as accountants, solicitors, business advisors and consultants;
- suppliers and other third parties with whom we have commercial relationships, for business, marketing, and related purposes;
- primary schools, Department of Education and other relevant community organisations for the purposes of school readiness reports, information sharing and support for your child;
- information sharing under the Family Violence Information Sharing Scheme as permitted under Part 5A of the Family Violence Protection Act 2008 and the Child Information Sharing Scheme as permitted under the Child Wellbeing and Safety Act 2005.
- any organisation for any authorised purpose with your express consent.

We may combine or share any information that we collect from you with information collected by any of our related bodies corporate (within Australia).

Direct marketing materials

We may send you direct marketing communications and information about our services and products that we consider may be of interest to you. These communications may be sent in various forms, including mail, SMS, fax and email, in accordance with applicable marketing laws, such as the Spam Act 2003 (Cth). If you indicate a preference for a method of communication, we will endeavour to use that method whenever practical to do so. In addition, at any time you may opt-out of receiving marketing communications from us by contacting us (see the details below) or by using opt-out facilities provided in the marketing communications and we will then ensure that your name is removed from our mailing list.

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

We do not provide your personal information to other organisations for the purposes of direct marketing.

How can you access and correct your personal information?

You may request access to any personal information we hold about you at any time by contacting us (see the details below). Where we hold information that you are entitled to access, we will try to provide you with suitable means of accessing it (for example, by mailing or emailing it to you). We may charge you a fee to cover our administrative and other reasonable costs in providing the information to you and, if so, the fees will be a fee unit in line with government recommendations (currently equal to $15.00) per half hour or part thereof to a maximum of $117.80 per request. We will not charge for simply making the request and will not charge for making any corrections to your personal information.

There may be instances where we cannot grant you access to the personal information we hold. For example, we may need to refuse access if granting access would interfere with the privacy of others or if it would result in a breach of confidentiality. If that happens, we will give you written reasons for any refusal.

If you believe that personal information we hold about you is incorrect, incomplete or inaccurate, then you may request us to amend it. We will consider if the information requires amendment. If we do not agree that there are grounds for amendment then we will add a note to the personal information stating that you disagree with it.

What is the process for complaining about a breach of privacy?

If you believe that your privacy has been breached, please contact us using the contact information below and provide details of the incident so that we can investigate it.

Do we disclose your personal information to anyone outside Australia?

We may disclose personal information to our related bodies corporate and third party suppliers and service providers located overseas for some of the purposes listed above. We take reasonable steps to ensure that the overseas recipients of your personal information do not breach the privacy obligations relating to your personal information. We may disclose your personal information to entities located outside of Australia, including the following:

• our related bodies corporate;

• our data hosting and other IT service providers, located in the United States and Philippines; and

• other third parties located in the Philippines.

Security

We take reasonable steps to ensure your personal information is protected from misuse and loss and from unauthorised access, modification or disclosure. We may hold your information in either electronic or hard copy form. Personal information is destroyed or de-identified when no longer needed.

As our website is linked to the internet, and the internet is inherently insecure, we cannot provide any assurance regarding the security of transmission of information you communicate to us online. We also cannot guarantee

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

that the information you supply will not be intercepted while being transmitted over the internet. Accordingly, any personal information or other information which you transmit to us online is transmitted at your own risk.

Data Breaches and Responding to Data Breaches

What is a data breach?

A data breach occurs when there has been unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information. Some examples included:

- **bestchance** mistakenly providing personal information to the wrong person by sending details to the incorrect email or mailing address
- lost or stolen laptops, removable storage devices or paper records containing personal information.
- databases containing personal information being "hacked" into or otherwise illegally accessed by individuals outside of the agency or organisation
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure recycling or garbage bins

Responding to data breaches

Each breach will need to be dealt with and responded to on a case by case basis. **bestchance** will undertake an assessment of the risks involved, and accordingly decide what actions to take in the circumstances. We take each situation seriously and will act quickly to assess and contain the breach.

Containing the breach

If a data breach is discovered or suspected, immediate steps will be taken to limit the breach. The breach must be escalated internally to the respective General Manager and the Privacy Officer, and in consultation with the Quality and Risk Manager.

Evaluating the risks associated with the breach

To determine whether **bestchance** will need to notify the relevant parties and inform them of the next steps, there will be an assessment whether serious harm is likely. The following factors will be considered:

- *The type of information involved*: some information is more likely to cause serious harm if compromised, whether that harm is physical, financial or psychological. For example, driver's licence, health and financial account details may pose a greater risk of harm to an individual than their name or

address. Also, a combination of personal information typically creates a greater risk of harm than a single piece of personal information.

- *Circumstances of the data breach*: **bestchance** will consider whose personal information was involved in the breach, how long the information was accessible for, whether it was encrypted or anonymised; as well as assessing which parties have gained unauthorised access to the information.
- *The nature of the harm:* **bestchance** will consider the broad range of harms that may result from the data breach. Some examples may include identity theft, significant financial loss by the individual, loss of business or employment opportunities, humiliation, damage to reputation or relationships.
- *The cause and extent of the breach:* the cause of the breach is an important factor as the risk may be less where the breach is unintentional or accidental, rather than intentional or malicious. **bestchance** will consider whether the personal information has been recovered, whether there is a systemic issue and how many individuals are affected by the breach when making an assessment.

Notification

Following the assessment, the Privacy Officer in consultation with the Quality and Risk Manager will decide whether the data breach is considered eligible in accordance with the Notifiable Data Breach scheme. An eligible data breach arises when the following three criteria are satisfied:

1. There is unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information that bestchance holds,
2. this is likely to result in serious harm to one or more individuals, and
3. **bestchance** has not been able to prevent the likely risk of serious harm with remedial action.

If **bestchance** has reasonable grounds to believe an eligible data breach has occurred, we will promptly notify individuals at likely risk of serious harm. The Office of the Australian Information Commissioner (the Commissioner) must also be notified as soon as practicable. If this is the case, **bestchance** will notify:

- all individuals to whom the relevant information relates, or
- only those individuals at serious risk, or
- publish a notification

The notification to affected individuals and the Commissioner will include the following information:

- **bestchance**'s identity and contact details
- a description of the data breach
- the kinds of information concerned, and

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

- recommendations about the steps individuals should take in response to the data breach

Preventing future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, **bestchance** will take actions that are proportionate to the significance of the breach, as well as investigate whether it was a systemic breach or an isolated event.

Records management

Human Resources (Staff) Records:

- Records are maintained in both hard and electronic copy including the Human Resource Information System, as follows but not limited to:
    - Details of recruitment and selection
    - Professional qualifications and relevant Licences, for example, Working with Children, VIT Registrations, and current Victorian Driver's Licence
    - Payroll related records
    - Performance and professional development information
- Any staff records will not be destroyed until a minimum of seven years following employment termination.
- Only access the personal, sensitive or health information of an individual when directly relevant to their primary area of work.

Volunteers' Records

- Records are maintained in both hard and electronic copy and will include, but not limited to:
    - Details of recruitment and selection
    - Personal and contact details
    - Any relevant qualifications and relevant licences, for example, Working with Children or current Victorian Driver's Licence

Donors' Records

- Personal information is collected and used by staff involved in the management of the fundraising function for the purposes of eliciting, processing, receipting, and acknowledgement of donations. This occurs with the informed consent of the donors.

Vendors and Contractors' Records

- Personal information which includes, but is not limited to: Working with Children and Police Records Checks, evidence of insurances and references, may be required. The information collected is used to verify suitability in providing services to **bestchance.**

Table of Disposal/Destruction Dates

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

	Record/File Type	Disposal/Destruction Date
1	Pre-Recruitment and Recruitment records Staff	Recruitment records are stored for a period of up to four weeks Minimum 7 years after employment termination The practice at **bestchance** is to keep the records for a minimum 30 years due to portability of Long Service Leave for Kindergarten based staff. Incident reports will be retained in perpetuity.
2	Volunteers	Minimum 7 years after conclusion of volunteering
3	Children – Kindergartens, Long Day Care and Family Day Care • Enrolment, incident and injuries • Medication • Attendance	• 25 years after child leaves service • 3 years after the child's last attendance • 7 years after the child's last attendance
4	Burwood Boy's Home	No disposal date, and to be retained by bestchance
5	Donors	No specific date but records will be retained by bestchance
6	Vendors and Contractors	No specific date but records will be retained by bestchance
7	Students	30 years after completion of course

Staff members will:

- Appropriately and securely store all personal, sensitive and health information.
- Only access the personal, sensitive or health information of an individual when directly relevant to their primary area of work.
- Only share personal, sensitive or health information with other staff members when required to do so in carrying out their usual and required work.
- Operate in accordance with parental consent in relation to the use of images and/or visual recordings of children.
- Electronic records containing personal, sensitive and health information will be stored securely and only accessed by authorized personnel with a password.

Links

Our website may contain links to other websites operated by third parties. We make no representations or warranties in relation to the privacy practices of any third party website and we are not responsible for the privacy policies or the content of any third party website. Third party websites are responsible for informing you about their own privacy practices.

Contacting us

Date Created	27 April 2016
Date Reviewed	28 August 2019
Review Date	3 Years

If you have any questions about this privacy policy, any concerns or a complaint regarding the treatment of your privacy or a possible breach of your privacy, please use the contact link on our website or contact our Privacy Officer using the details set out below. We will treat your requests or complaints confidentially. Our representative will contact you within a reasonable time after receipt of your complaint to discuss your concerns and outline options regarding how they may be resolved. We will aim to ensure that your complaint is resolved in timely and appropriate manner.

Please contact our Privacy Officer at:

Privacy Officer
Bestchance
Post: 2/254 Canterbury Road Bayswater North
Tel: 03 8562 5100
Email: privacy.officer@bestchance.org.au

Complaints can also be directly submitted to the Office of the Victorian Privacy Commissioner on 1300 666 444 or enquiries@cpdp.vic.gov.au

Changes to our Privacy Policy

We may change this privacy policy from time to time. Any updated versions of this privacy policy will be posted on our website. This privacy policy was last updated on 28 August 2019.