Data Protection and Information Governance Policies

Confidential Documents

No information should be kept about a young person that they have no knowledge about; a young person must have access on request to this information. Confidential documents should be kept in a locked file the keys to this file should only be accessible to the worker involved. Files can only be removed from the premises with a Police warrant or at request of line manager through certain circumstances.

Data Protection

- The data protection act 1998 applies to both paper and computer files.
- No information about a person should be kept without their knowledge and they have access to that information.
- Confidential documents should be kept in a locked file. The keys to this file should only be accessible to the worker/ workers involved.
- Files kept on a computer or in a filing cabinet are subject to the Data Protection Act.
- Files can only be shared with the person's permission apart from certain circumstances for example, disclosure to authorities, legal adviser or as required by law.
- Files can only be removed from premises with a Police warrant or at the request of a senior member of the organisation in special circumstances.
- Personnel records must be kept for 6 years unless otherwise determined by a third party with a vested interest.

GDPR

General Data Protection Regulation (GDPR), applies to employees, contractors and agency staff. It covers personal data we collect and use on paper and electronically including our databases, paper records, video and photographs, voice recordings and mobile devices such as laptops, mobile phones and memory sticks.

The law gives individuals (data subjects) several rights to control personal information and how it is used by us. The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (the right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Communications provided to the data subject concerning any of the rights detailed in this procedure must be clear and transparent using plain language. If any communications are sent to a child, you must ensure that they are written in such a way as to make them easily understandable by the child.

Where communications are received electronically responses should be made by electronic means wherever possible unless the data subject requests otherwise.

Response Times

If a data subject makes a request to us about any of the rights in relation to any personal information, we hold about them, we normally have 1 month to respond to the request. Where we decide not to action a request, we must inform the requestor why we are not actioning the request and advise them of the right to complain to the Information Commissioner's Office.

The Right to be Informed

When we collect information from individuals (or their representative) we must be clear about what we are going to do with that information. We must tell them what we will use their data for, how long we will keep it, who we may share it with, and the other details listed below.

This information is usually provided in a Privacy Notice. The information in the notice must be concise, transparent, intelligible, easily accessible and written in clear and plain language. Where information is addressed to a child, it must be written in such a way that they can easily understand.

The Right of Access

Individuals have the right to ask for copies of personal information Invictus Wellbeing Services CIC holds about them. This is called a Subject Access Request.

Individuals should be asked to provide proof of their identity. If you need to verify the identity of an individual, you can ask them for any evidence you reasonably need to confirm it.

Subject Access Requests

An individual is entitled to all the information we hold about them. Information about third parties (anyone other than the requestor) should be removed unless the requestor would already know this information, or the requestor provides the other persons consent to disclose their information. There are some circumstances where the information will be exempt from the right of subject access. For example, if the disclosure would prejudice a criminal investigation.

This policy statement came in to force on: **11/03/20**

The policy statement and accompanying procedures were last reviewed on:

Signed: D. Hutchinson

Print: D. Hutchinson

Date: **11/03/21**