Name of Charity: Time 4 Children.

Time 4 Children is registered with the Charity Commission. Charity Registration Number: 1111837

On the 25th May 2018 the General Data Protection Regulation came into force.

The Data Protection Act 1998 requires every data controller who is processing personal information to register with the Information Commissioner's Office (ICO). Time 4 Children is a data controller.

Data Controller

Time 4 Children complies with the GDPR and is registered as a 'Data Controller' with the Information Commissioner's Office.

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

The Data Protection Officer (DPO) for Time 4 Children is Mrs A Pithie (Trustee).

ICO Reference Number: ZA366888

DATA PROTECTION/PRIVACY POLICY

The Trustees for Time 4 Children, herein referred to as T4C, are ultimately responsible for ensuring that personal data shall be processed lawfully, fairly, is accurate, is kept secure and is retained for no longer than is necessary.

The Trustees intend to comply fully with the requirements and principles of the Data Protection Act 1984, the Data Protection Act 1988 and General Data Protection Regulations 2018.

Staff involved with the collection, processing and disclosure of personal data, are aware of their duties and responsibilities within these guidelines. Enquiries Information about T4C's Data Protection Policy is available from the T4C. General information about the Data Protection Act can be obtained from the Information Commission Office (0303 123 1113) https://ico.org.uk/

T4C undertakes to inform all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection forms.

Processing means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

Data subject means an individual who is the subject of personal data or the person to whom the information relates.

Personal data means data, which relates to a living individual who can be identified by name, address, telephone number, email address and photographs if published in the press, Internet or media.

Parent has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

Registered Purposes

Registered purposes covering the data held at the charity are listed on T4C's registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data Integrity

T4C undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs T4C of a change of circumstances, their computer record will be updated as soon as is practicable.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, T4C will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Data we collect, why and retention times.

Data held about staff, Trustees and volunteers will not be kept for longer than necessary for the purposes registered. It is the duty of the DPO to ensure that obsolete data are properly erased. All personnel records are stored in a secure yet easily accessible area, for the following lengths of time:-

<u>One Year</u>
Staff, Trustees and Volunteer records

<u>Two Years</u>
Any pay-related records, such as earnings and pay rates

<u>Three Years</u>
Payroll records and all paperwork related to Family or Medical Leave

<u>Five Years</u>
Any information, including a summary of details, pertaining to an occupational injury or illness. However any medical exams that are required by law because of the occupational injury or illness will be kept for 30 years.

Personnel Records will be checked for irrelevant data annually by a senior office staff member and checked with the DPO.

The following documents are kept in the employee/volunteer personnel file:-

- Job Description
- Job Application
- Offer of employment
- Copy of contract of employment including terms and conditions, pay, hours of work, holidays, benefits, absence
- Receipts for Child Protection
- Any performance evaluations given
- Any accidents connected with work
- Emergency contact details

After 5 years T4C will hold summary details for reference purposes which will include Name, DOB, dates of service and reference recommendation

Children's Data

T4C receives personal data from referrals; parent/main carer consent information. This data is stored securely* and will not be passed on to third parties. Exception: Child Protection concern/disclosure.

<u>Seven Years</u>

Records relating to children are kept securely for seven years after Time 4 Children have lost contact with the child as per NSPCC guidelines. This allows for future subject access. *By securely we mean all paper records will be scanned and held digitally on secure sharepoint.*

Children's session records are kept securely* in order to monitor children's progress by Lead and Senior Practitioner to determine length of time support is required.
Information about child protection concerns and referrals are kept securely* in a separate child protection file for each child. As per NSPCC guidelines, T4C is a voluntary organisation and therefore where such further intervention has been necessary records relating to child protection are kept for 7 years after T4C's last contact with the child, or where necessary case notes are passed onto Social Services and not retained by T4C.

Exceptions:

In some cases, records are kept for longer periods of time. For example, if: the records provide information about a child's personal history, for example a looked after child might want to access at a later date; the information in the records is relevant to legal action that has been started but not finished; or the records have been archived for historical purposes (for example if the records are relevant to legal proceedings involving the organisation). Where there are legal proceedings legal advice will be sought about how long to retain records.

When records are kept for longer than the recommended period, files will be clearly marked with the reasons for the extension period and stored securely.*

Destruction of child protection records

When the retention period finishes, confidential records will be shredded in the presence of a member of the organisation by an entrusted firm specialising in the destruction of confidential material. Any electronic versions of the record will be purged. If not shredded immediately, all confidential records must be held in a secured plastic bag, labelled as confidential and locked in a cupboard or other secure place.

If T4C closes down, arrangements will be made for the on-going management of records. This includes the review, retention and disposal of records.

Twenty Five Years

A Child Protection allegation record made against any staff member, volunteer or Trustee for T4C, complaint or legal action record in accordance with T4C's insurance policy will be securely* stored for twenty five years or until normal retirement age, whichever is the sooner. (NSPCC guidelines)

T4C will keep records for the same amount of time regardless of whether the allegations were unfounded. However if it found that the allegation is malicious, the record will be destroyed immediately. (NSPCC guidelines)

T4C must keep any records that could be needed by an official inquiry (for example the Independent Inquiry into Child Sexual Abuse (IICSA, 2017). Inquiries will issue directions for records to be retained and these must be followed.

Subject Access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

For children under the age of consent, access is obtained from whoever holds parental responsibility for the child.

T4C's policy is that:

Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

When a request is made for any information regarding a child, be it from a parent, school or authority, a security question will be asked of the individual to give dob of child and or another piece of data to ensure the dialogue is with regard to the data subject.

Processing Subject Access Requests

Requests for access must be made in writing. Parents, staff, volunteers or authorities may ask for a Data Subject Access form, available from the T4C office. Completed forms should be submitted to the DPO at T4C.

Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type

of data required (e.g. Child's Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date).

Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be dated on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 working days.

Authorised Disclosures

T4C will, in general, only disclose data about individuals with their consent. However there are circumstances under which T4C's authorised officer may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:

- Child data disclosed to authorised recipients in respect of Child Protection, a child's health, safety and welfare.
- Staff/volunteer data disclosed to relevant authorities eg in respect of a complaint and administrative matters.
- Unavoidable disclosures, for example, to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a confidentiality form promising not to disclose the data outside the Charity.

T4C will initiate a process for phone calls and emails whereby it asks for a security check, e.g. asks individual to give dob of individual and or another piece of data to ensure the dialogue is with regard to the data subject.

Disclosure and Barring Checks

T4C will not store copies of disclosure and barring check certificates. A confidential record will be kept of: the date the check was completed; the level and type of check (standard/enhanced/barred list check and the relevant workforce) and the reference number of the certificate; If there is a dispute about the results of the check, a confidential record will be kept of: the date the check was completed; the level and type of check (standard/enhanced/barred list check and the relevant workforce) and the reference number of the certificate and the decision made about whether the person was employed/volunteer (with reasons).

If there is a dispute about the results of a check, T4C may keep a copy of the certificate for not longer than 6 months. NSPCC guidelines.

Computer Security

T4C undertakes to ensure security* of personal data. Security software is installed on all computers containing personal data. Secure encrypted hard drives. Secure Office 365 (Sharepoint) cloud storage with automated backups. Advanced mailboxes in secure Office 365 (Exchange) email accounts. In order to be given authorised access to the computer staff undergo checks and sign a confidentiality agreement. Only 3 authorised users are allowed access to the computer files and password changes are regularly undertaken.

Physical Security

Appropriate building security measures are in place by office landlord.

Logical Security

Volunteer Practitioners using own computers/laptops to type children's session notes must delete notes once submitted to the Practice Manager. Volunteer Practitioners must delete for ever children's session notes submitted by email. Volunteer Practitioners must not identify a child in any way in session notes or emails. Volunteer Practitioners are not allowed to retain any information regarding a child.

Procedural (Operational) Security

All staff, volunteers and Trustees understand their Data Protection obligations and their knowledge is updated as necessary.

Computer printouts as well as source documents are disposed by an approved data shredding company. Overall security policy for data is determined by the Board of Trustees and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data within T4C should in the first instance be referred to the DPO.

Individual members of staff, volunteers or Trustees can be personally liable in law under the terms of the General Data Protection Regulations. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data.

Media/Marketing Communications

Media communications will only be handled by the nominated media lead, Chairperson or the Trustees.

Media communications about Time 4 Children are clear, consistent and positive. Should the media approach a Trustee, volunteer or employee regarding Time 4 Children, no comment will be given until appropriate approval has been sought and approved.

Time 4 Children will not pass onto any third parties personal data for marketing purposes. Permission to opt in will be sought to circulate materials containing information about Time 4 Children, such as newsletters, fund raising events. For the purpose of raffle prizes where contact details are taken, contact details will be destroyed immediately after a draw has taken place.

A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from T4C's DPO.

T4c has a complaints policy on request.

A personal data request form can be requested from:

Time 4 Children

Email: office@time4children.org.uk

Date of issue: 15/05/2018
End date: 14/5/2024