EXTRATIME Data Policy

1. INTRODUCTION

Extratime is committed to protecting your privacy. This policy explains how and why we collect and use personal information about yourself, your child(ren) and others involved in their care. We recommend that you read this policy in full, but if you do not have time, the main points are:

- Your data is collected so that we can share information about Extratime services, events, fundraising activities. Personal data relating to children and young people using Extratime services and their families is necessary for us to provide appropriate care and support.
- We collect the minimum amount of data we need in order to do this.
- Your data is stored electronically on secure, password protected computers and within Extratime's cloud based storage. Paper records are in locked filing cabinets.
- We keep your data as required by law and in accordance with a file retention plan.
- We are careful to ensure that we only retain data and contact people who would reasonably expect to hear from us; for example, if they existing or potential Extratime service users, staff and volunteers, or people who have attended or expressed an interest in Extratime events or fundraising activities.
- You can ask for your details to be removed from our mailing lists at any time. You are also entitled to a copy of the data we hold about you.
- We will never sell, rent or otherwise distribute or make public your personal information

By using our website, any of our services, or providing us with any personal information we will assume you are agreeing to your information being used and disclosed in the ways described in this policy.

RELEVANT LEGISLATION

The personal data collected, stored and used by Extratime is done so in accordance with relevant national and international legislation with regards to data protection and user privacy:

- UK Data Protection Act 1988 (DPA)
- EU Data Protection Directive 1995 (DPD)
- EU General Data Protection Regulation 2018 (GDPR)

GDPR

The **EU General Data Protection Regulation (GDPR)** effective from May 2018 gives all EU citizens more rights and protections for their personal data, to minimise the possibility of theft and fraud.

These regulations include provisions for the following areas:

- **The right to be informed:** ***Companies must publish a privacy notice, in addition to explaining transparently how they use this personal data.***

- **The right of access:** ***Individuals will have the right to demand details of any of their data that a company may hold. This information must be provided within one month of request and there will normally be no charge to the individual.***
- **The right to rectification:** ***If a person's data is incorrect or incomplete, he or she has the right to have it corrected. If the company that holds the information has passed any of that information to third parties, the company must inform the third party of the correction and inform the person which third parties have their personal data.***
- **The right to be forgotten:** ***A person may request the removal of his or her personal data in specific circumstances.***
- **The right to restrict processing:** ***Under certain circumstances, an individual can block the processing of his or her personal data.***
- **The right to data portability:** ***A person can access their data for their own use anywhere they prefer.***
- **The right to object:** ***A person can object to the use of their personal data for most purposes.***

1.0 OUR CORE PRINCIPLES REGARDING USER PRIVACY AND DATA PROTECTION

- User privacy and data protection are inviolable human rights.
- We have a duty of care to people contained within our data
- Data is a liability: it should only be collected and processed when absolutely necessary
- We will never sell, rent or otherwise distribute or make public your personal information

Extratime also applies the principles of GDPR to the protection of personal data that it holds.

- Data is processed lawfully, fairly and in a transparent manner.
- Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected.
- Data accurate and, where necessary, kept up to date.
- Data is kept in a form which permits identification of data subjects for no longer than is necessary.
- Data is protected in a manner that ensures appropriate security of the personal data.

1.2 Definitions

'Data Subject' – an individual who is the subject of personal data.

'Personal Data' – information about a living individual (the 'Data Subject') who can be identified from that information.

'Data' – information recorded in manual or computerised form. This can include data held partly on computer files and partly on manual files providing that, when these are taken together, the subject of the data can be identified. It can mean data on computers, mobile phones and photo copiers.

'Relevant Filing System' – any set of information structured by reference to individuals, or by reference to criteria relating to individuals, in such a way that particular information relating to a particular individual is readily accessible.

'Sensitive Data' – amongst other items this can include data regarding subject's racial or ethnic origins, political opinions, religious or other beliefs, trade union membership, physical or mental health, sexual life and the commission or alleged commission of any criminal offences.

'Data Controller' – The Act requires the organisation/charity to be appointed as the 'controller' and a person appointed as the nominated Data Protection lead. Extratime is the nominated controller, and the Chief Executive Officer (CEO) is the nominated Data Protection lead. The Chief Executive Officer (CEO) has overall responsibility for a compliance with the Data Protection Act (DPA). The CEO should ensure creation, implementation and annual review of a Data Protection Policy (DPP) and related policies, processes and procedures. Day to day monitoring of the compliance could be delegated to senior managers, trustees, staff and members, but responsibility for information risk remains with the CEO.

2. POLICY

2.1 Confidentiality

Personal data is confidential and will be disclosed only for registered purposes to charity staff and other agents of Extratime when carrying out their work, to others as detailed in the appropriate registration, and to a court under the direction of a court order. Staff whilst aiming to provide appropriate support to children, young people and families, will not offer absolute confidentiality as there may be circumstances as outlined in 5.3 below, when it is impossible to do this.

2.2 Design of Computerised and Manual Record Systems

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third party data processor if they have agreed to comply with these procedures and policies, or if adequate measures have been put in place by themselves. Computer and manual record systems and files will be designed to comply with the Data Protection principles, which are as follows:

The information to be contained in personal data shall be obtained, and the personal data shall be processed, fairly and lawfully. Personal data shall be held for specified and lawful purposes only. Personal data shall be accurate and, where necessary, kept up to date. Where there are concerns over the accuracy of data it should not be used. Personal data held for any purpose or purposes shall not be kept for longer than is necessary.

Security of Information

Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data. Appendix 1 is a guidance sheet on how to protect data stored on equipment.

2.3 Registration

It shall be the responsibility of the Data Controller to maintain the register entry of Extratime with the Office of the Information Commissioner (ICO).

Information regarding new systems or files or new uses of existing files shall be provided to the Data Controller in sufficient time to enable amended registration details to be submitted before the new system is brought into use.

2.4 Unregistered Personal Data

Unregistered or inaccurate personal data will not be held. The Data Controller may examine any data to determine the accuracy of registration and staff must co-operate in this process. If unregistered personal data is detected it shall not be processed further until registered or, if it is held for an inappropriate purpose it should be disposed of.

2.5 Quality and Currency of Personal Data

Extratime will hold the minimum data necessary to enable it to perform its business. The data will be deleted once the need to hold it has passed. This stipulation shall, however, be subject to the specific requirements of the CEO, auditors and other bodies who may require data to be held to facilitate the closing or audit of Extratime accounts or the inspection of services.

Every effort will be made through staff induction and training to ensure that data is accurate and up-to-date, and that inaccuracies are corrected without unnecessary delay. To this end employees and all data subjects are required to keep Extratime informed of any changes in their personal circumstances, e.g. marital status, address, telephone numbers, next of kin etc.

Personal data shall be processed fairly and lawfully and shall not be processed unless at least one of the following conditions is met:

a) Data subject's consent is given
b) It is necessary for the performance of a contract or with a view to entering into a contract
c) There is compliance with the data controller's legal obligations (but not imposed by contract)
d) It is in the Data subject's vital interests
e) It is required for the Administration of justice
f) It is in the Data Controller's legitimate interests – must not prejudice rights and freedoms of the data subject and must inform the data subject at the time of collection the purpose for processing and the legitimate interest it is relying on to process the data
g) A safeguarding referral is required. Refer to Extratime Safeguarding children and young people policy.

If processing sensitive personal data one of the following conditions also have to be met:

a. Explicit consent
b. Data controller's legal right/obligation in connection with employment
c. To protect vital interests of a data subject (where consent cannot be give/obtained)
d. Legitimate interests of not for profit organisations
e. Data subject has already made public

f. Legal proceedings
g. Administration of justice

2.6 Access Rights for Data Subjects

Extratime will make all reasonable efforts to ensure that data subjects are aware of the data which is kept about them, where it is kept and why it is kept. Extratime will provide access to any individual who requests access to their data in a reasonable manner.

If the information to be provided to a data subject identifies another person in addition to the data subject, the information will not be disclosed unless and until the other person has given written authorisation for the disclosure to be made.

Applicants must supply sufficient information both to confirm their identities, and to locate the data sought. The response to the application will be met as soon as possible and in any case, within one month of the request. The one month period commences when Extratime receives sufficient information to respond to the data subject's request. Where requests are complex or numerous Extratime will be able to extend the response period by a further two months.

Personnel files are available for inspection by staff, upon advance written request and in the presence of the HR Lead or the Chief Executive Officer.

2.7 Disclosure of Personal Data

Extratime may disclose personal data if it is requested for any of the following purposes:

- Safeguarding Children and Vulnerable Adults cases
- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of any tax or duty

This is at the discretion of the CEO and no employee must take it upon him or herself to disclose personal data in any of the above circumstances, except when instructed to do so by a Court Order which has been validated by the Chief Executive or other member of the Management Committee, or when instructed to do so by a legal representative of Extratime. The only exception to this is where a child, young person is in immediate danger and to withhold information places them at risk. In these circumstances, the employee must use discretion and seek support from the most senior employee available.

2.8 Transmitting Data outside of the Organisation

Receiving data from external third party

Parent carers give permission for personal information relating to individual children and young people to be collected by Extratime from third parties. This is an important part of Extratime's needs and risk assessment process and ensures we are aware of and able to fully support children and young people in our care.

Sending data to external third party

Any requests for personal data from a third party should only be shared with written permission from Extratime CEO or HR Lead. Permission must be requested using the form provided in Appendix 1.

Data may only be sent or received using the following process;

- Third parties include local authorities, schools, colleagues and community and voluntary sector partners.
- Requests for information should include a scanned copy of the parent carer permission section of the booking form
- Be addressed to the appropriate named individual
- Sent by secure email
- Information received must be stored in accordance with Extratime's data sharing, retention and storage policy
- Email must be deleted as soon as it has been saved to the appropriate secure location
- Any physical data must be sent by recorded delivery, by special delivery or by courier in order that it is possible to obtain a receipt to track delivery.

Sharing data within Extratime

Wherever possible personal data should only be shared using Sharepoint, the shared drive. Memory sticks must not be used to store of share personal data. Where Sharepoint is not available and / or where paper records are shared, security and confidentiality must be considered at all times. Where paper records are transported between the office and venues, they must be taken directly from one venue to another in a private or Extratime vehicle only. They should be stored securely immediately upon arrival.

Wherever possible, paper records must not be taken to external meetings. Instead records should be accessed electronically from Sharepoint or arrangements should be made with the meeting host to share records.

3. DATA SUBJECT CONSENT

Extratime respects peoples' preferences on how they wish to be contacted and what they wish to hear from us about. We only contact people that have actively opted in to hear from us. We will respect these choices until the data subject chooses to opt out.

If the data subject makes a donation to Extratime or attends an event, we may contact them with other opportunities to support or donate – this is in line with the guidelines on legitimate interest. If the data subject requests not to be contacted regarding further opportunities to donate, Extratime will respect these choices.

If a parent/carer registers with Extratime the organisation will be able to send them any information relating to bookings and schemes.

When an individual expresses an interest in becoming an employee of Extratime we will send them information relating to employment opportunities. Once recruited, we will contact staff about employment opportunities and other matters relating to their employment at Extratime

4. WHAT TO DO IF DATA IS LOST OR RELEASED

Appendix 4 is a guidance sheet on how to protect data stored on equipment.

However, a data security breach can happen for a number of reasons:

- Loss or theft of equipment containing data
- Inappropriate access and poor controls or human error
- Hacking or Phishing of blagging offences

In these cases it is important that the organisation should

- Contain the source of the data loss and seek to recover any lost data
- Access the data loss and consider the on-going risk
- Notify the Information Commissioner's Office, other regulators and the data subject within 72 hours of a breach. The data subject does not need to be informed if the breach is unlikely to result in a risk to the data subject. High risk is typically measured as the likelihood fraud will be committed with the leaked information or that publication of the data could cause the data subject extreme distress or embarrassment.
- Evaluate the loss and consider how it can be prevented from re-occurring
- All data losses whether actual or suspected of both electronic and /or paper based information should be immediately reported to the CEO. (The nominated Data Protection Lead.)

See Appendix 5 for the steps to follow in the event of a breach or if you suspect a breach may have happened.

5. POLICY & DATA TRAINING REVIEW

This policy will be reviewed annually, to take account of changing legislation, organisational needs and trends in best practice. Employees and volunteers will receive raining on a regular basis on the importance of Data Protection, and is included in the Safeguarding training for all employees. Changes to this policy will be informed to employees as soon as possible and certainly no later than our weeks after effect. This is of importance as indefinite retention is unsustainable and legislative changes need to be reflected in the policy.

6. DATA COLLECTION, STORAGE AND RETENTION

Please see separate Data collection, storage and retention policy for full details on how Extratime collets, uses, stores and how long it keeps personal data.

7. DATA DESTRUCTION

Information held for longer than is necessary carries additional risk and cost. Records and information should only be retained for legitimate business use. Under the DPA 1998, personal data processed by Extratime should not be retained for longer than is necessary for its lawful purpose.

Data reaching its retention period should be reviewed on a regular basis, preferably each quarter and then signed off for destruction by the CEO who will ensure that the destruction request is in line with the retention period required by the relevant class of data.

Storage and destruction of records can be undertaken by third parties contracted for those purposes. There should be no paper documents disposed of that have not been shredded first. Processes must be in place to ensure that all backups and copies are included in the destruction of records.

8. RIGHT TO E RASURE (RIGHT TO BE FORGOTTEN)

Any data subject has the right to have their personal data erased without undue delay. This right is contingent on the occurrence of one of the following:

- The data is no longer necessary
- The data subject withdraws consent
- The data controller has no overriding grounds for continuing the processing against the objection
- Processing was unlawful
- Erasure is necessary for compliance with EU or national law
- The individual object to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data is processed in relation to the offer of information society services to a child.

Extratime can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- Archiving purposes in the public interest, scientific research historical research or statistical purposes
- The exercise or defence of legal claims

Ends
25.5.18