GDPR DATA PROTECTION POLICY & PROCEDURES

1. General Statement:

The Let's Play Project is required to process **personal data** (Information by which an individual can be identified) regarding applicants, young people and families, donors, management, staff, trustees and other volunteers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

To achieve this, the Let's Play Project endeavours to comply with the General Data Protection Regulation (GDPR) which was introduced in May 2018 and has replaced the Data Protection Act 1998.

The Let's Play Project is registered with the **Information Commissioner's Office, registration number ZA519122.** Should you have any queries you may contact them on: 0303 123 1113. Information is available at www.ico.org.uk

The Let's Play Project has appointed Samantha Bates, Charity Manager, as their **Data Protection Controller**. If you have any questions with regard to your personal data or GDPR please call Sammy on 01295 810661 or email sammy@letsplaybanbury.org

2. Principles:

2.1. All trustees, management, staff, and other volunteers should be aware of the 6 GDPR principles and as far as is reasonably practicable ensure all personal data is:

2.1.1. **Lawful, fair and transparent**; *There must be legitimate grounds for collecting the data, the data collection must not have a negative effect on the person or be used in a way they wouldn't expect.*

2.1.2. **Limited for its purpose;** *Data must be obtained for specified & explicit purposes and only processed in accordance with those purposes. Not used in a way that someone wouldn't expect.*

2.1.3. **Adequate & Necessary**; *It must be clear why the data is being collected and what will be done with it. Unnecessary data or Information without any purpose should not be collected.*

2.1.4. **Accurate;** *Data must be kept up-to-date and changed if it is inaccurate*

2.1.5. **Not kept for longer than necessary;** *data should not be kept for longer than is needed, must be properly destroyed or deleted when no longer in use or goes out of date.*

2.1.6. **Integrity and confidentiality**; *data should be processed securely, with protection against unauthorised or unlawful processing, loss, damage or destruction and be kept safe and secure* Vulnerable adults are people who are over 18 years of age and are getting or may need help and services to live in the community. Vulnerable adults may be unable to take care of themselves and be unable to protect themselves from harm or exploitation by other people.

3. Personal Data

3.1. Personal data covers both facts and opinions about an individual. It includes information necessary for applicants, beneficiaries, donors, management, staff, trustees and other volunteers such as name, location data, identification number, online identifier; it may also include information about the person's health and appraisals.

3.2. Processing of Personal Data & Consent

3.2.1. Consent must be a positive indication. It cannot be referred from silence, inactivity or pre-ticked boxes.

3.2.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individuals wishes.

3.2.3. Where consent is given a record will be kept documenting how & and when consent was given.

3.2.4. Any information which falls under the definition of personal data will remain confidential and will only be disclosed to third parties with the

consent of the individual. Individuals must be informed of how their data is being used.

3.2.5. Individuals have the right to withdraw consent at any time.

3.2.6. A proper physical & technical security system must be used to keep personal information safe and secure, and not be exposed to undue security risks

3.3. Sensitive Personal Data

3.3.1. Let's Play may, from time to time, be required to process sensitive personal data regarding applicants, beneficiaries, leaders and trustees. Where sensitive personal data is processed by the Charity, the explicit consent of the individual will generally be sought in writing.

3.3.2. Sensitive personal data include:

a. Medical information

b. Religious or other beliefs

c. Education and training details

d. Family lifestyle and social circumstances

e. Financial details

f. Physical or mental health condition

g. The commission or alleged commission of an offence

3.4. Individual Rights

3.4.1. Individuals have the right to access to information held by Let's Play. Any individual wishing to access his/her personal data should make a ***Subject Access Request*** in writing via email or post to Sammy Bates, Data Protection Controller. Let's Play will respond to any written requests as soon as is reasonably practicable and within 30 days. Individuals also have the right to stop their personal data being used if it is causing distress via the ***Right to Restrict Processing***, prevent it from being used for direct marketing, have inaccurate data changed ***Right to Rectification***, and claim compensation for damaging data breaches. In certain cases,

individuals have the right to request that specific data be deleted or destroyed via the ***Right to Erasure***. Individuals can only request information relevant to themselves.

3.4.2. **The Let's Play Project has a responsibility to establish whether the information requested by an individual is relevant to the person requesting it.**

3.4.3. The ***Right to be Forgotten*** under GDPR means an individual can request that online content is removed from an organisations database. The ***Data Portability Act*** means that a person can request all their personal data be transferred to another system for free.

3.5. Accuracy

3.5.1. Let's Play will ensure that all personal data held in relation to applicants, beneficiaries, management, staff, donors, trustees and other volunteers are accurate. Individuals must notify the Data Protection Controller/Officer of any changes to information held about them. An individual has the right to request that inaccurate information about them be erased.

4. Data Protection Controller

4.1. Let's Play has appointed Sammy Bates, Charity Manager, as **Data Protection Controller** who will ensure that all personal data is processed in compliance with the principles of the GDPR.

4.2. In addition, Let's Play will ensure that:

4.2.1. Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.

4.2.2. Everyone managing and handling personal information is appropriately trained to do so.

4.2.3. Everyone managing and handling personal information is appropriately supervised.

4.2.4. Queries about handling personal information are promptly and courteously dealt with.

4.2.5. Methods of handling personal information are clearly described.

4.2.6. A regular review and audit is made of the way personal information is held, managed and used.

4.2.7. Methods of handling personal information are regularly assessed and evaluated.

4.2.8. Performance with handling personal information is regularly assessed and evaluated.

4.2.9. A breach of the rules and procedures identified in this policy by a member of staff is a potential breach of the Code of Conduct and may lead to disciplinary action being taken.

4.3. Enforcement:

4.3.1. If anyone believes that Let's Play has not complied with this Policy or acted in accordance with the GDPR, the individual should inform the Data Protection Controller/Officer appointed by Let's Play.

4.4. Information Security Policy:

4.4.1. Personal or sensitive personal data can only be disclosed to authorised persons on a need to know basis and with the consent of the individuals concerned.

4.4.2. No personal or sensitive personal data can be disclosed without authorisation from the Data Protection Controller

4.4.3. All nomination papers, additional information, interview notes etc. will be stored by named trustees and assessors at Let's Play and will only be accessible to authorised personnel. All information kept on authorised computers will be password-protected. Backup copies of information stored on computers will be made regularly and will be kept in the secure fire proof safe. Papers sent to interviewers must be kept in a secure place and only accessible to authorised personnel. All such papers will be collected in after the interviews and shredded.

4.4.4. Personal and sensitive personal data will only be kept as long as is necessary.

4.4.5. All personnel involved in any way with the handling of personal and sensitive personal data will be trained on Let's Play Project's data protection policies, security systems and procedures. All breaches of security will be investigated should they occur.

4.4.6. Any emails which contain sensitive or personal information as defined above will only be sent to the recipient via a secure email using Egress.

5. Protection of Personal Data:

5.1. The Let's Play Project is registered under the **Information Commissioner's Office No. ZA519122.**

5.2. Data Protection concerns safeguarding data about individuals to maintain their privacy, and good information management practice.

5.3. Data Protection covers "manual" records - including paper, microfilm, and other media as well as those processed by information technology of any kind.

6. Data Retention

6.1. The Let's Play Project will:

6.1.1. Not keep personal data longer than 6 months necessary

6.1.2. Delete personal data as soon as practicable

6.1.3. Paper documents will be burned or destroyed

7. Data Breach

7.1. A data breach refers to a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

7.2. Let's Play will ensure all staff understand and are made aware of what constitutes a breach as part of their training.

7.3. If a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. This should be within 72 hours of Let's Play becoming aware of the breach.

7.4. Within a breach notification the following information will be outlined;

7.4.1. The nature of the breach including categories and approximate numbers of individuals and records concerned.

7.4.2. The name and contact of the Data Protection Controller

7.4.3. An explanation of the likely consequences

7.4.4. Where appropriate a description of measures taken to mitigate any possible adverse effects.

Failure to report a breach may result in a fine as well as a fine for the breach itself.

Date of Policy – 1st September 2021

Signed …….. Chair of Trustees

Signed …….. Operations Manager

Signed …….. Activities Manager

Registered Charity No. 1180524

Review Date – 1st November 2023