Registered Charity No. 1180524

GDRP, Data Handling & Safer Recruitment Policy

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 Sammy Bates 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 info@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*data should not be kept for longer than is needed, must be properly destroyed or deleted when no longer in use or goes out of date.*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.

2.1.7. **Be held securely.** *Data will be in held securely and only accessed by authorised personnel for the express purposes for which it has been collected.*

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, date of birth, identification number, online identifier; it may also include information about the person's health and appraisals.

3.2. How we will use the data we collect

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

I. Where we need to perform the contract we have entered into with you.

II. Where we need to comply with a legal obligation.

III. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

I. Where we need to protect your interests (or someone else's interests).

II. Where it is needed in the public interest [or for official purposes].

3.3. Processing of Personal Data & Consent

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

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

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

3.3.4. 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.

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

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

3.4. Sensitive Personal Data

3.4.1. 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.

3.4.2. 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

3.5. Individual Rights

3.5.1. 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 Tracey Owen, 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.

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

3.5.3. 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.

3.6. Accuracy

3.6.1. 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. DBS & Safer Recruitment Data Handling

2.1. In line with local authority guidelines, the Let's Play Project will follow new statutory legislation introduced to ensure that safe recruitment practice is carried out.

2.2. As a first step, all persons showing an interest in working or volunteering at the Let's Play Project will be required to sign an in-house Declaration form in advance - this is not a replacement for the enhanced DBS disclosure).

2.3. The Disclosure and Barring Service (DBS) provides criminal record disclosures for those working with young people.

2.4. The Let's Play Project requires that applications be made to the DBS for all employees, trustees and volunteers for an enhanced DBS disclosure who are aged 16 and over.

2.5. All applicants for volunteer and Playworker vacancies will be given a Staff Suitability form (Disqualification by Association) to fill out prior to the interview – any issues raised on the form will be discussed at the interview and necessary advice from external agencies will be taken.

2.6. It is essential that safe recruitment practice is in place to ensure that unsuitable persons do not gain access to work with young people either on a paid or voluntary basis.

Procedures

3.1. DBS procedure for employees, trustees, volunteers working with the Let's Play Project:

3.1.1. The Activities Manager (or another senior appointed person) will ask if the new candidate is already signed up to the DBS update service.

3.1.2. If they are signed up to the DBS update service, a member of the Core Staff team will carry out a Status check at www.gov.uk/dbs, after viewing the original DBS Certificate and record necessary information as stated in 2.3.

3.1.3. If the person is thought to be suitable to join the Let's Play Project, then at the second interview stage they will be asked to bring along documents that are needed for our own new enhanced DBS disclosure, this will apply to all persons aged 16 or above who wish to be involved in the Let's Play Project even if a person has an existing enhanced DBS disclosure elsewhere (unless they have signed up to the DBS update service).

3.1.4. If the existing disclosure highlights 'convictions' or 'other matters,' then a risk assessment is required, and a record kept. In this case refer to the Let's Play Project's own policy regarding the employment of ex-offenders (PP04) and as a safeguard, seek advice from the Local Authority for guidelines.

3.1.5. Upon return of the DBS form to the new employee, Let's Play will ask for the employee to bring their DBS form into the office, if the new disclosure has 'convictions' or 'other matters' revealed, then the Let's Play Project Activity Manager must carry out a risk assessment (as above). If the employee refuses to bring in their DBS form, we cannot employ them.

3.1.6. No one may work directly with Young People without a current and satisfactory enhanced DBS disclosure which has been applied for through the Let's Play Project unless they are signed up to the online update service.

3.2. DBS Procedure for placement students:

3.2.1. The Activities Manager (or other senior appointed person) will contact the College Work Placement Officer before the placement student

starts their placement at Let's Play to confirm they have a current up to date enhanced DBS.

3.2.2. The Work Placement Officer will then have to provide a letter to Let's Play detailing:

a. Full Name of Placement Student

b. Date of Issue on DBS form

c. DBS Number

3.3. Recording procedure and tracking

3.3.1. The date the DBS application is sent will be recorded.

3.3.2. A follow-up online tracking of the application may be required if there is a delay in its return.

3.3.3. The Let's Play Project's in-house tracking form will record details of all enhanced DBS Disclosures, including:

a. Full Name

b. Date of Issue

c. DBS number

d. Disclosures – 'convictions' or 'other matters'

e. Expiry date – 3 years from date of issue to be noted (renewal).

3.3.4. These will be held in a secure file in the office.

3.3.5. The Let's Play Project will renew all enhanced DBS disclosures every 3 years.

3.3.6. Further information about DBS checks is available at: https://www.gov.uk/disclosure-barring-service-check/overview

5. How we use sensitive personal data

Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. Where we need to carry out our legal obligations or exercise rights in connection with employment.

2. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities

6. Data Protection Controller

6.1. Let's Play has appointed Tracey Owen, Operations Manager, as **Data Protection Controller** who will ensure that all personal data is processed in compliance with the principles of the GDPR.

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

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

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

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

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

6.2.5. Methods of handling personal information are clearly described.

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

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

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

6.2.9. 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.

6.3. Enforcement:

6.3.1. 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.

6.4. Information Security Policy:

6.4.1. 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.

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

6.4.3. 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.

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

6.4.5. 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.

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

7. Protection of Personal Data:

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

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

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

8. Data Retention

We have put in place measures to protect the security of your information. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

9. Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or

reporting requirements. In order to determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

10. Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact [POSITION] in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. In order to withdraw your consent, please contact your Manager in writing (including the legal basis for your belief that your consent can be withdrawn). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify

you in other ways from time to time about the processing of your personal information.

11. Data Breach

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

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

11.3. 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.

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

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

11.4.2. The name and contact of the Data Protection Controller

11.4.3. An explanation of the likely consequences

11.4.4. 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 – 31st May 2023

Signed …….. Chair of Trustees

Signed …….. H&S Trustee

Signed …….. Data Controller

Review Date – 31st May 2024

Please note this policy supercedes:

PP05 Secure Storage & Handling of disclosures

PP06 DBS & Safe Employment

PP22 GDPR Data Protection