



<b>Company Name:</b>	STAMP UK Ltd
<b>Document</b>	Data Protection Policy and Procedure
<b>Topic:</b>	Data protection (GDPR)
<b>Date:</b>	02/09/2020
<b>Review Date:</b>	01/09/2021

## Contents

- Introduction
- Definitions
- Data *processing* under the Data Protection Laws
  1. The data protection principles
  2. Legal bases for processing
  3. Privacy by design and by default
- Rights of the Individual
  1. Privacy notices
  2. Subject access requests
  3. Rectification
  4. Erasure
  5. Restriction of *processing*
  6. Data portability
  7. Object to *processing*
  8. Enforcement of rights
  9. Automated decision making
- Personal data breaches
  1. *Personal data breaches* where the Company is the *data controller*
  2. *Personal data breaches* where the Company is the *data processor*
  3. Communicating *personal data breaches* to individuals
  
- The Human Rights Act 1998
- Complaints

## Appendix

Annex – legal bases for processing personal data

---

All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their *personal data* whilst imposing certain obligations on the organisations that process their data.

This policy sets out how the Company implements the Data Protection Laws. It should be read in conjunction with the Data Protection Procedure.

In this policy the following terms have the following meanings:

**'consent'** means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of personal data relating to him or her;

**'data controller'** means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*;

**'data processor'** means an individual or organisation which processes *personal data* on behalf of the *data controller*;

**'personal data'**\* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal data*;

**'processing'** means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**'sensitive personal data'**\* means *personal data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions. [Note 1]

\* For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we specifically need to refer to *sensitive personal data*.

**'Supervisory authority'** means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is [the Information Commissioner's Office](#) (ICO).

**All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.**

The Company may hold *personal data* on individuals for the following purposes:

- 
- Staff administration;
  - Direct communication with an individual for the purpose of advertising, marketing and public relations
  - Accounts and records;

### **1. The data protection principles**

The Data Protection Laws require the Company acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that *personal data* that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the *personal data* are processed;
6. Processed in a manner that ensures appropriate security of the *personal data*, including protection against unauthorised or unlawful *processing* and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

### **2. Legal bases for processing**

The Company will only process *personal data* where it has a legal basis for doing so. Where the Company does not have a legal reason for *processing personal data* any processing will be a breach of the Data Protection Laws.

The Company will review the *personal data* it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

### **3. Privacy by design and by default**

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities. This includes implementing measures such as:

- data minimisation (i.e. not keeping data for longer than is necessary);
- anonymization
- cyber security

The Company shall provide any information relating to data *processing* to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

---

**Subject access requests** The individual is entitled to access their *personal data* on request from the *data controller*

#### **1. Rectification**

The individual or another *data controller* at the individual's request, has the right to ask the Company to rectify any inaccurate or incomplete *personal data* concerning an individual.

#### **2. Erasure**

The individual or another *data controller* at the individual's request, has the right to ask the Company to erase an individual's *personal data*.

#### **3. Restriction of processing**

The individual or a *data controller* at the individual's request, has the right to ask the Company to restrict its *processing* of an individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes its erasure;
- The Company no longer needs the *personal data* for the purposes of the *processing*, but the *personal data* is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

#### **4. Data portability**

The individual shall have the right to receive *personal data* concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *data controller* in circumstances where:

- The *processing* is based on the individual's *consent* or a contract; and
- The *processing* is carried out by automated means.

Where feasible, the Company will send the *personal data* to a named third party ONLY on the individual's request.

#### **5. Object to processing**

The Company shall cease *processing* unless it has compelling legitimate grounds to continue to process the *personal data* which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their *personal data* for direct marketing.

#### **6. Enforcement of rights**

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

---

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

## **7. Automated decision making**

The Company will not subject individuals to decisions based on automated *processing* that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is authorised by law; or
- The individual has given their explicit *consent*.

The Company will not carry out any automated decision-making or *profiling* using the *personal data* of a child.

### **Reporting *personal data* breaches**

All data breaches should be referred to the persons whose details are listed in the Appendix.

#### **1. *Personal data* breaches where the Company is the *data controller*:**

Where the Company establishes that a *personal data breach* has taken place, the Company will take steps to contain and recover the breach. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the *personal data breach* happens outside the UK, the Company shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

#### **2. *Personal data* breaches where the Company is the *data processor*:**

The Company will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

#### **3. Communicating *personal data* breaches to individuals**

Where the Company has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.

The Company will not be required to tell individuals about the *personal data breach* where:

- The Company has implemented appropriate technical and organisational protection measures to the *personal data* affected by the breach, in particular to make the *personal data* unintelligible to any person who is not authorised to access it, such as encryption.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

---

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life.
- Freedom of thought, belief and religion.
- Freedom of expression.
- Freedom of assembly and association.
- Protection from discrimination in respect of rights and freedoms under the HRA.

If you have a complaint or suggestion about the Company's handling of *personal data* then please contact the person whose details are listed in the Appendix to this policy.

Alternatively you can contact the ICO directly on 0303 123 1113 or at <https://ico.org.uk/global/contact-us/email/>

NAME	POSITION	CONTACT NO
Susannah Moody	Company Director	07957215965

The Company provides Drama Clubs to school age children. The Company must process personal data (including sensitive personal data) so that it can provide these services – in doing so, the Company acts as a data controller.

You may give your personal details to the Company directly, such as on an application or registration form or via our website. The Company must have a legal basis for processing your personal data. We will only use your personal data in accordance with the terms of the following statement.

## 1. Collection and use of personal data

### Purpose of processing and legal basis

The legal bases we rely upon to offer these services to you are:

- Your consent
- Where we have a legitimate interest
- To comply with a legal obligation that we have
- To fulfil a contractual obligation that we have with you

## 2. Data retention

The Company will retain your personal data only for as long as is necessary for the purpose we collect it.

Where the Company has obtained your consent to process your [personal/[and] sensitive personal data/specify which personal data], we will do so in line with our retention policy [(a copy of which is attached)]. Upon expiry of that period the Company will seek further consent from you. Where

---

consent is not granted the Company will cease to process your [personal data/[and] sensitive personal] data].

### **3. Your rights**

Please be aware that you have the following data protection rights:

- The right to be informed about the personal data the Company processes on you;
- The right of access to the personal data the Company processes on you;
- The right to rectification of your personal data;
- The right to erasure of your personal data in certain circumstances;
- The right to restrict processing of your personal data;
- The right to data portability in certain circumstances;

### **4. Complaints or queries**

If you wish to complain about this privacy notice or any of the procedures set out in it please contact: Susannah Moody 07957215965 or by email on [susannah@stampdrama.co.uk](mailto:susannah@stampdrama.co.uk)

You also have the right to raise concerns with Information Commissioner's Office on 0303 123 1113 or at <https://ico.org.uk/concerns/>, or any other relevant supervisory authority should your personal data be processed outside of the UK, if you believe that your data protection rights have not been adhered to.