# Story Films
## Data Protection Policy - Requirements for all Staff 2023

## 1. PURPOSE AND SCOPE

Story Films strongly values the importance of the privacy of its staff, contributors and all those involved in the creation, production and distribution of its world class content. When people entrust us with their personal information we must only ever use it in ways which they are comfortable with. This policy sets out those procedures and measures that all personnel engaged by Story Films must follow and take in order to protect all Personal Data collected, stored or otherwise processed in the course of their duties and to ensure our compliance with the Data Protection Act 1998 and all other applicable data protection legislation.

We expect all staff to comply with this policy regardless of the country in which they work and/or any local laws that may provide for a less stringent level of protection. Any breach of or non-compliance with this policy may result in disciplinary action up to and including dismissal.

Breaching data protection rules can also lead to substantial reputational damage to Story Films and significant fines as well as significant harm to the individuals whose data has been mismanaged.

This policy does not form part of any individual's contract of employment and it may be amended at any time.

## 2. RESPONSIBILITY

All staff must, as soon as possible at the beginning of their engagement, read and understand this policy.

All staff must throughout their engagement with Story Films comply with the terms of this policy and immediately alert their Data Protection Officer, or if not available, their line manager, if they become aware of a possible data security breach or a breach of this policy.

If you have any questions or concerns regarding this policy or data protection compliance generally, please contact your Data Protection Officer. **Your Data Protection Officer is Josh Wilkins, COO at Story Films**

## 3. DEFINITIONS

**It is essential that you understand the following key definitions used in this policy:**

"**Personal Data**" means any information about an identified or identifiable person. A person is identifiable if he/she can be identified directly or indirectly from that information or from that information used in conjunction with any other information which may include names, addresses, images, telephone numbers, personal email addresses, dates of birth, bank and pay roll details, next of kin, IP addresses and any information automatically collected when using computers and the internet.

"**processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure (including by transmission, dissemination or otherwise making available), alignment or combination, blocking, erasure or destruction.

**These definitions are very wide and, as such, it is extremely likely that you will process Personal Data as part of your role and that, as a result, this policy is directly applicable to you.**

Examples of processing Personal Data include:

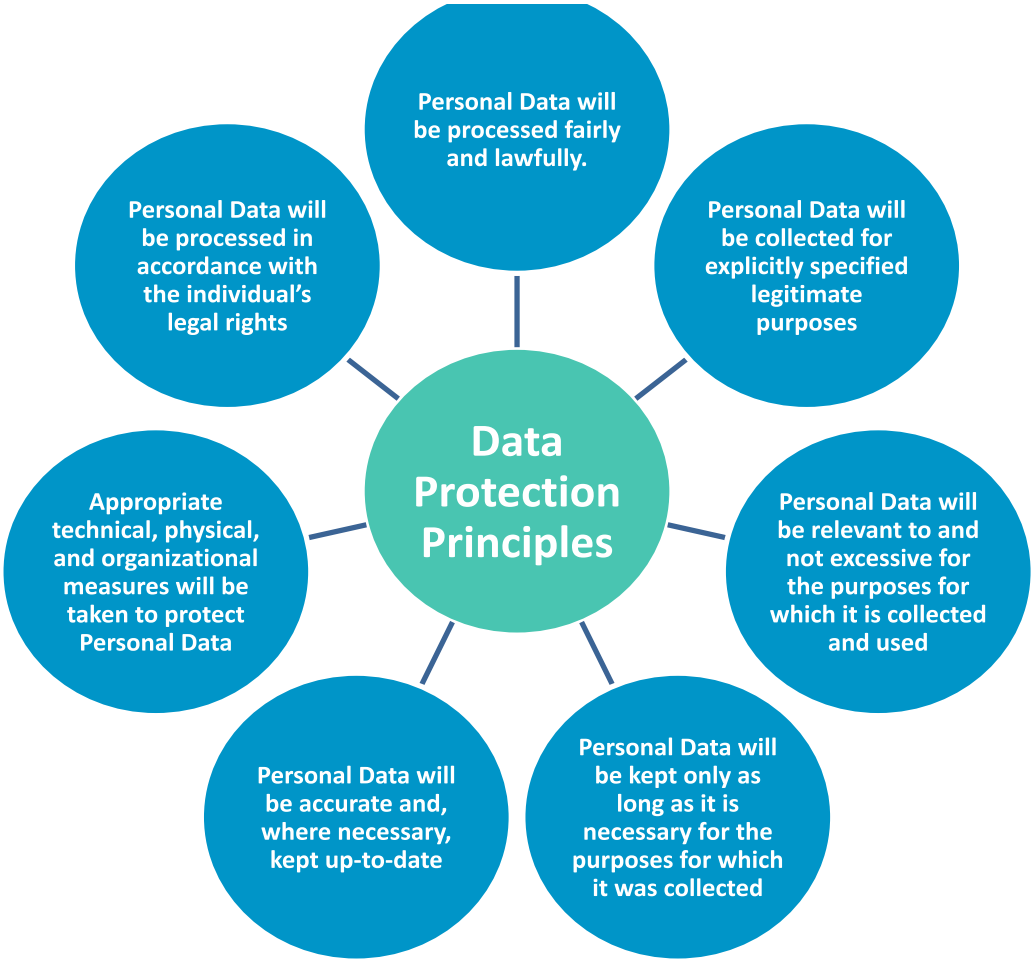
1. Recording a contributor's name and address following a phone call;
2. Filming (even if not intended for broadcast) and storing footage;
3. Storing a contributor questionnaire which has been sent by email;
4. Printing out and distributing call sheets.

In addition, always be aware what constitutes "**Sensitive Personal Data**". Sensitive Personal Data means any data that relates to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health matters, sexual orientation/life, alleged or actual criminal activity and criminal records.

**When Personal Data is also Sensitive Personal Data, you MUST ALSO COMPLY with Part 6 of this policy.** This includes notifying your Data Protection Officer before processing any such data.

## 4. DATA PROTECTION PRINCIPLES

When processing Personal Data, all staff must comply with the Data Protection Principles set-out below:



## 5. COLLECTION OF AND ACCESS TO PERSONAL DATA

Subject to certain exceptions, **you can only collect Personal Data which you have the data subject's permission to collect and you must only use Personal Data for the limited purposes for which the Personal Data was collected.**

You will have access to and/or will routinely acquire Personal Data in many forms and from many sources, including but not limited to correspondence, phone calls, call sheets, filming and storing footage, invoices, lists of employees and may be in hard copy or soft copy.

You must limit the collection of Personal Data to what is actually and likely to be needed. For example, in the context of a production, it is not necessary to collect details of an individual's age or occupation or sexual orientation unless this is relevant to the programme.

When collecting Personal Data you must tell the individual who you are, why you are collecting their Personal Data and how their Personal Data will be processed. The individual must then consent to the collection and processing of their data in that way. You do not need to provide any information which is clearly obvious, but if you are in any doubt, it is always better to provide too much information. Where possible, this consent should be **express written consent** to the collection and processing of Personal Data. Express written consent may be contained in a questionnaire or release form and should explicitly refer to how that individual's data will be processed. If obtaining express written consent is not possible, you should instead obtain oral consent. The consent must accurately reflect how you will be processing the Personal Data.

**Personal Data must then only be used for those purposes for which it was collected and consent was given.**

Generally, you **must** have the **express written consent** of the data subject to process their data before **any** filming (even if not intended for broadcast). The **only** exception is the processing of personal data related to the filming of passers-by when filming in public (remember – simply capturing someone's image constitutes processing their personal data). In these circumstances (and as long as no further personal data is processed) consent can be implied so long as appropriate industry-standard measures (such as filming notices) are in place.

You must also ensure the Personal Data you keep about an individual is accurate and up-to-date, recognising that an individual has the right to access copies of any Personal Data that is held about them and to request its correction or deletion.

**If you want to use Personal Data for marketing, speak to your Data Protection Officer first.**

## 6. PROCESSING OF SENSITIVE PERSONAL DATA

Where you are collecting and/or processing confidential and/or Sensitive Personal Data:

A. you must always **notify** your Data Protection Officer before processing Sensitive Personal Data and comply with any additional procedures or obligations required by him; and
B. you must always obtain the **express written consent** of the individual prior to processing their Sensitive Personal Data. This involves explaining to the data subject exactly what data will be processed and how it will be processed before asking for their consent.

Sensitive Personal Data should **not be taken off-site or transported or transmitted** except with the express prior permission of your Data Protection Officer.

Special care must always be taken when disclosing Sensitive Personal Data. You must ensure that only the intended recipient receives the information. When sending Sensitive Personal Data by email, you must **only include the data in password-protected attachments** and communicate the password by separate means (for example by phone).

Sensitive Personal Data must **only be stored online within a password-protected subfolder** which you will be directed to by your line manager.

## 7. KEEPING PERSONAL DATA SECURE

**All Personal Data must be stored and transported securely.**

**The following measures provide an absolute minimum of measures for keeping electronic equipment on which Personal Data is stored or transported secure:**

A. Do not use your own equipment for storing Personal Data; only use devices and equipment provided by Story Films.
B. Passwords for all devices (e.g. laptops, PCs, memory sticks), files and your email account must be kept secure and confidential and changed regularly and must not be shared with anyone.
C. Your line manager will tell you where and how you can save Personal Data electronically. Never save Personal Data anywhere else.
D. Memory sticks containing Personal Data must be held on a keyring or lanyard and kept on your person at all times, not stored in bags or left in vehicles.
E. Any device that is lost must be reported immediately to IT (as well as to your Data Protection Officer in line with this policy) so they can perform a remote wipe of the device.
F. Ensure that your PC always automatically locks after 10 minutes, with the network password needed to unlock them.
G. Ensure that your work Blackberry, iPhones and other mobile devices are always password-protected and auto-lock after 5 minutes.
H. Paper documents containing Personal Data must be stored securely and not left on view. Unnecessary copying of paper and electronic records must not be undertaken. Freelancers are not permitted to take crew lists from job to job.
I. Personal Data must not be given to any third party (either verbally or otherwise) without the express written permission of the data subject unless required to do so by a legitimate authority (e.g. the police). Great care should be taken when dealing with people claiming to be from some kind of authority. Proof needs to be obtained of a person's identity before any information is disclosed to them. All such requests must be authorised by your company Data Protection Officer or line manager. You should suggest that the person making the oral request put their request in writing if you are not sure about the caller's identity. Don't be afraid to ask for assistance in difficult situations. No-one should be bullied or harassed into disclosing Personal Data.
J. Every template document (e.g. contributor questionnaires) must be double checked to ensure that it is a clean template prior to it being emailed to potential contributors. Always save contributor templates as "read only".

K. Always use your company email account. Never send Personal Data to your personal email account. Always double-check recipients and email addresses before sending any emails containing Personal Data.

## 8. TRANSPORTING PERSONAL DATA

Physical transportation of paper and electronic files between the office and location (or anywhere else) and back should, wherever possible, be avoided as there is always a risk of data being lost or stolen in transit.

Only use reputable couriers for sending devices or documents containing Personal Data. **Do not send them by post.**

## 9. TRANSFERRING PERSONAL DATA TO OTHER COMPANIES

Any transfer of Personal Data between Story Films and a third party (including All3Media Head Office) must be solely for the purposes of that third party performing the services they have been contracted to perform. Where Personal Data is to be transferred to a third party, Story Films must require the third party to comply with this policy or to guarantee the same levels of protection as this policy when dealing with Personal Data.

**You should always consult with your Data Protection Officer prior to the transfer of Personal Data to another company (including All3Media Head Office) even if you have the express written consent of the data subject.**

## 10. RETENTION AND DISPOSAL OF PERSONAL DATA

**Personal Data should not be kept longer than is necessary** and if the data is no longer relevant for the purpose for which it was obtained, the data should be securely destroyed.

Accordingly:

A. printed material containing Personal Data should be securely destroyed using the confidential bins provided (if your company does not provide confidential bins consult your line manager or Data Protection Officer about how to destroy paper copies securely);
B. CD's, tapes and all other media must be wiped before recycling; and
C. if you are reusing media, including tapes, DVD's and memory sticks they should be completely wiped before they are 'written over'.

## 11. WHAT TO DO IN THE EVENT OF A DATA SECURITY BREACH

**It is imperative that all actual or suspected data security breaches and breaches of this policy are notified <u>immediately</u> to your Data Protection Officer.** If he is not available, contact Pete Beard or Dave Nath.

A data security breach is any incident involving unauthorised access, disclosure or loss of Personal Data. Non-exhaustive examples of data security breaches are:

A. the loss or theft of computer hardware, data sticks, media hard drives, paper files, tapes, disks or any other medium that contains Personal Data; and
B. the inadvertent disclosure of an individual's Personal Data to a third party not entitled to receive such Personal Data (for example, by sending an email containing an individual's Personal Data to the

wrong recipient or verbally disclosing an individual's Personal Data to a third party without the individual's knowledge or consent).

## 12. DATA SUBJECT ACCESS REQUESTS

Any data subject is entitled to enquire as to the nature of the Personal Data stored or processed about them by any company. **If you receive such a request, do not respond and forward the request to your Data Protection Officer.**

## 13. CHANGES TO THE DATA PROTECTION POLICY

Story Films reserves the right to change or replace this Data Protection Policy at any time. Any such changes will be notified to you by Story Films and should be carefully reviewed so that you are at all times familiar with the version of this policy which is in force.

**March 2023**