Data Protection

BIG MOUNTAIN PRODUCTIONS LTD DATA PROTECTION POLICY

The Data Protection Act 2018 and the General Data Protection Regulations in force in accordance with this Act has an impact on us all: - as well as the more obvious examples like how to protect data held on laptops and memory sticks, it also covers issues such as the handling of requests from callers to reception for private mobile phone numbers and how to manage personal information produced on call sheets or displayed on PC screens around the office and rushes containing interviews and CCTV.

All employees and workers will be required to acknowledge that they have read and agree to abide by the guidelines contained in this policy. **Contravening the Act, in certain cases, is a criminal offence that can be punishable by an unlimited fine in the Crown Court and liability for damages.**

Whilst every employee and worker is responsible for data protection, the designated Responsible Person(s) in accordance with the Data Protection Act 2018 are Jane Kelly and Denise Fogarty. In the first instance, if you have any issues, doubts or questions regarding Data Protection please speak with your line manager immediately upon becoming aware of the same.

IF ANYONE BECOMES AWARE OF ANY POSSIBLE BREACH OF THIS GUIDELINE, PLEASE ALERT YOUR LINE MANAGER IMMEDIATELY.

1. Introduction

Everyone has rights with regard to how their personal information is handled. In the course of business, employees and workers store and process certain types of personal information and we recognise the need to treat it in an appropriate and lawful manner. Personal Data **(as defined below)** includes, for example, data that identifies current, past and prospective employees, programme contributors, contractors and suppliers and others with whom companies within the Group conducts business or otherwise communicate with.

The Act sets out the legal framework for the handling of personal information that identifies living people. All

organisations that hold or process Personal Data must comply with the law and this policy aims to assist the Group companies in managing and processing data in accordance with the Act.

It is essential that you read and understand this policy document and what is required of you.

1.1 What is Personal Data?

The Act applies to all Personal Data. Personal Data is data which identifies a living individual when combined with other information, for example a name and a phone number. Personal data can be factual or it can be an opinion. Some types of Personal Data are defined in the Act as being 'Sensitive' and can only be processed under
strict conditions, and will usually require the express permission of the individual concerned.

Personal Data

This includes: personal information/data that identifies a living individual by that personal information/data such as names, addresses, telephone numbers, mobile phone numbers, personal email addresses (if it includes
the person's name), dates of birth, agent details, next of kin, bank or building society details, employment history/CV, passport information, payroll/fee information, performance appraisal.

Sensitive Personal Data

This includes: medical information (including physical or mental health or condition), references from previous employers, any information on minors (i.e. anyone under the age of 18), membership of trade unions, information on an individual's sexual orientation and/or sexual life/race or ethnic origin/religious or similar beliefs/political opinions, personality/psychometric tests, criminal convictions.

Sensitive Personal Data can only be collected, processed and used under strict conditions, and will usually require the express consent of the individual concerned.

Processing

This includes: any activity that involves the use of the data. It includes obtaining, recording or holding the

data,

or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. It also includes transferring personal data to third parties.

Personal Data including Sensitive Personal Data as defined by the Act is routinely included in, but is not limited to, programme scripts, treatments, briefs, running orders, invoices, purchase orders, float and expenses claims, company bank statements, call sheets, company organigrams, lists of employees and payroll/fee information. In other words, care needs to be taken when handling data which is very much part and parcel of your everyday

work practices.

For personal data to be processed lawfully, certain conditions have to be met. These are described in more detail in the next sections and may include, among other things, requirements that the individual has consented to the processing, or that the processing is necessary for the legitimate interest of the date controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the individual's consent to the processing of such data will be required (unless otherwise approved by HR and/or the Data Protection Officer).

a. **1.2 What are our obligations?**

The Act sets our eight key principles regarding the processing of personal data. Personal Data must be –

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. 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."

1.3 What we have to do

In simple terms, we need to make sure that the Personal Data we gather and use is:

• kept safe;

• used only for the purpose for which it was gathered;

• used by you properly when performing your normal work duties;

• accurate and kept up to date;

• kept no longer than necessary and disposed of in the correct way; and

• in the case of Sensitive Personal Data, in most cases this use must be with the consent of the individual concerned (unless otherwise approved by HR and/or the Data Protection Officer).

2. Policy Statement

It is our policy to:-

1. only collect, handle, process, store, record, use, transport, and retain Personal Data that is necessary for the company to conduct its business,
2. respect the privacy of individuals; and
3. ensure that any Personal Data held is secure, giving access only to those who have a lawful right to access. This applies to both automated and manual records.

3. Policy

Company Policy for the areas is set out below and must be followed by all employees and workers.

• Data Records

• Verbal Communication

• CCTV Systems

• Buildings and Premises

• Key Departments

• Data Disposal

• **Laptops, portable media and the use of data offsite.**

• Data Monitoring/Review

• Data Breaches

• Data Requests

Data Records (for example paper records, emails, electronic files stored on computers or portable memory

devices, rushes, audio, video)

Data records are any media which may contain personal information. For example, they could be paper contracts, spreadsheets, rushes with captions, or sound recordings. Great care and attention should be paid to them by all employees and workers.

• Paper documents containing Personal Data must be stored securely and not left on view. Accordingly, appropriate measures need to be undertaken to ensure that no day to day paper records are left unattended

so that they might be seen by visitors unauthorised to view them. A ‘Clean Desk’ policy should be operated, with all paperwork and files to be locked away outside normal office hours.

• Unnecessary copying of paper and electronic records must not be undertaken. For example does a call sheet really have to be duplicated and distributed to so many people?

• Special care should be taken when ‘faxing and emailing Sensitive Personal Data. You need to ensure that only the intended recipient receives the information. Passwords must be used on documents and communicated by phone to the recipient of sensitive emails.

• Special attention must be taken when constructing and presenting ‘pitch’ documents to broadcasters and partners. These documents must follow all of the guidelines set out in this document.

• Documents containing Personal Data must be shredded in a secure manner

• Electronic documents must be password protected or encrypted if they contain personal data. Passwords must only be made available to those authorised to process an individual’s information as is reasonably necessary.

• PC Network log-on passwords and email passwords must be made known only to authorised people

• PCs must be set to lock to screensavers if not in use for 10mins, with the network password needed to unlock them.

• Access to computer data must be limited to levels of the internal company system relevant to the particular

member of staff.

Verbal communication

Verbal communication of Personal Data must only be given to authorised individuals. For example, the disclosure

of personal email address, home phone numbers and home addresses must not be given out by anybody without

the express permission of that person. Great care should be taken when dealing with people claiming to be from

some kind of authority, for example the police. Proof needs to be obtained of that person's identity before any information is disclosed. All such requests must be authorised by your company Data Controller or line manager. You should suggest that the person making the verbal 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 information.

Buildings and Premises

Access to the building(s) must be controlled with appropriate and practical measures to protect Personal Data acquired by the Company.

If any of the following security measures are implemented, best practice would include the following:-

• swipe card entry systems which should be regularly monitored to ensure that only current members of staff have access to the building(s).

Notwithstanding the use of the measures above, where possible a clean desk policy must be implemented outside office hours **& it is crucial that any rushes are locked away in the locked edit suite or lockable drawers**

or cupboards before you leave at night.

3.6 Key Departments

Production Teams: production data must be kept in a separate PM folder for each programme. Access to this folder and data contents must be strictly controlled and be limited to the people working on that production

and to senior management. Any Sensitive Personal Data must be stored within a subfolder of the production folder and must be further secured by passwords and be available to a very limited access list. This access list must be reviewed at each production meeting by the production manager.

Production teams working on site must have a system of tracking original rushes and associated scripts and production paperwork back to the company's premises, to and from edit, to and from broadcasters on completion.

Business Affairs, HR, Accounts, IT: data is kept on a separate drive on the company's network and/or software

system. Access to this data is strictly controlled. Access to the departmental data must be limited to the people working in that department. Any Sensitive Personal Data must be secured further by passwords and a very limited access list. The access list must be reviewed regularly by the MD.

. **Data**

Disposal

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 destroyed.

Accordingly:-

- Printed material containing Personal Data should be securely destroyed,
- CD's, tapes and all other media must be wiped locally before recycling.
- If you are reusing media, including tapes, DVD's and memory sticks they should be completely wiped before they are 'written over'.

- IT departments must have a clear work process for dealing with old PCs, laptops and servers, which must have their hard drives wiped, tested and recycled or physically destroyed at the end of their useful life.

Laptops, portable media and the use of data offsite.

Personal Data **MUST** be kept secure.

The following must be complied with by, for example, staff who need to work from home or for on location.

The following practices should be adopted:-

- Sensitive Personal Data should only be taken off-site with the express permission of your line manager. All staff who work from home/on location must adopt the same policies with electronic and paper records as they do in the office.
- to remove the need to take personal data off-site, the Company has made it possible for staff to use a computer to access data remotely, when working away from the office.
- physically transporting paper and electronic files between the office and home/location and back should, wherever possible, be avoided as there is always a risk of data being lost or stolen in transit.
- any documents containing Personal Data must be, at the very least, password protected before being sent by email.
- any Personal Data downloaded to a portable memory device e.g. USB sticks, CD's, DVD's, Laptops, must be protected by a password, kept securely **AND** encrypted. USB sticks should be held on a keyring or lanyard and be kept on your person at all times and not stored in bags or left in vehicles. Encrypted sticks can be provided by your IT department.
- blackberry, iPhones and other mobile devices MUST be protected with a password that auto-locks after 30 minutes. Any device that is lost must be reported immediately.
- External Hard Drives used for data storage and rushes must be password protected when they contain personal data. An example of one such device would be the LaCie d2 Biometric SAFE Hard Drive range.

Please also remember that personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data. .

Data Monitoring/Review

Data must not be kept any longer than necessary, and must be kept secure, up to date and processed in accordance with the purpose that it was obtained.

- Production set up meetings - Production Managers/Executive Producers must specifically address the issue of data protection during the production process i.e. what Personal Data needs to be acquired, who should have access to it, etc.

Data Breaches

- It is imperative that any breaches or suspected breaches are dealt with straight away.
- For example; breaches of security could be the loss or theft of computer hardware, data sticks, media hard drives, paper files, tapes, disks or any other medium that contains Personal Data.
- A written assessment should be made of the incident that has occurred and the possible implications stated
- Arrangements will then be made to advise those affected as soon as it is practical to do so, in order that they can take any measures needed to protect themselves.

3.11 Links to general and more detailed advice

The following link to the Information Commissioner's Office web home page provides detailed information for best practices to a large range of departments and circumstances and is an excellent point of reference. https://ico.org.uk/

The http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 is also available for more detailed information.