Data Protection and Data Security Guidelines

Introduction:

In the course of our productions and general business activities we will collect, store and process personal data. Please see the Glossary at the back for key definitions.

Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties. Handling this data appropriately will maintain confidence in the company and will provide for successful business operations.

These data protection and security guidelines are designed to provide practical advice to assist in protecting us from civil and/or criminal sanctions and reputational damage as a result of an unauthorised use of, damage to, or loss or disclosure of personal data.

It is therefore important that all senior personnel read these guidelines and that the necessary practical support and guidance is provided for all production personnel.

Please also see the company's Data Protection Policy, Corporate Privacy Notice, Website Privacy Notice and any production-specific privacy information.

There are certain exemptions available under data protection legislation for journalism purposes /artistic purposes. However these exemptions do not dispense with the need to generally comply with data protection legislation. [Add link to ICO / PACT guidance on the new exemptions when available.]

1. Administration of Policy

On each production, the production manager will be the senior person within the company that has responsibility for data protection policy and practice on that production, with legal advice and assistance provided by the Production Lawyer. Any questions about data protection matters on an individual production should be referred to the Production Manager and Production Lawyer in the first instance.

The Tinopolis Group Data Protection Manager, has overall responsibility for data protection policy and practice for the company. Any data protection queries which cannot be answered by the Production Manager and Production Lawyer should be escalated to the Tinopolis Group Data Protection Manager, Sara Bond on Sara.Bond@Tinopolis.tv

Production Start Up

At the start of each production the Production Manager will arrange a meeting to review the scope of personal data management with the Production Lawyer (and the executive producer if appropriate) by completing the Data Protection Checklist. This will enable us quickly to review the types of data likely to be sourced for each production and agree safe processes to collect, store, distribute and dispose of them specific to each production. It will also enable us

to undertake a careful review of whether the personal data is necessary / proportionate for the programme for which it is being collected, to consider appropriate retention periods and to check that the processing of the personal data does not result in a high risk to the rights and freedoms of individuals.

As part of this process the Production Lawyer will work with the Production Manager / Executive Producer to create the following which meets the needs of each individual production:

- *A bespoke Production-specific Privacy Statement for the production based on the GDPR-compliant template*
- *Data protection wording for inclusion in research interviews, contributor searches, any and all advertising, application forms – will include a link to the production privacy policy*
- *Data protection wording for inclusion in contributor release forms – with a link to the website privacy notice*
- *Data protection wording for inclusion in freelancer contracts – with a link to the corporate privacy notice*

In addition, the Production Manager will create a Data Management Plan setting out details of the flow of personal data, who will have access to the personal data at the company, whether any third parties will have access to the personal data and the suitable controls that are in place, how it will be stored safely, who it will be distributed to and what safety measures will be in place and what will be retained / for how long and what will be destroyed at the end.

A copy of the completed Data Protection Questionnaire, Production-specific Privacy Statement and Data Management Plan will be provided to the Tinopolis Group Data Protection Manager for reference.

2. Data Protection Principles and Compliance Notes

Whenever we process personal data as a data controller, we must comply with the data protection principles. These state that personal data must be:

(a) processed lawfully, fairly and in a transparent way.

(b) collected only for valid purposes that have been explained to the data subject and not used in a way that is incompatible to those purposes,

(c) relevant and limited only to those purposes;

(d) accurate and kept up to date;

(e) kept only for as long as necessary for the purposes the data subject has been told about; and

(f) kept securely.

Please see the below practical notes:

A) Processed lawfully, fairly and in a transparent way

Personal data must be processed fairly and without adversely affecting the rights of the data subject and on the basis of one of the legal grounds set out in data protection legislation. We must ensure the data subject is made aware of what data is being collected / processed, for what purpose, who is carrying out the processing, how long the personal data will be held and the legal grounds for processing etc.

Action

Ensure all contributors receive a copy of the production-specific privacy statement before any personal data is collected / processed and include a link to the website privacy notice in all application forms / casting mail outs / research interviews etc

Ensure all contributors who are to appear in the production sign a contributor release form which includes a copy / link to the website privacy notice and the production-specific privacy statement which provides details of what personal data we are collecting / processing, for what purpose, who is carrying out the processing, retention periods, the lawful grounds for processing etc

B) Collected only for valid purposes that have been explained to the data subject and not used in a way that is incompatible to those purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted under law. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs and we need to ensure we have a valid legal ground for processing the data for the new purpose. In some circumstances, this may require a new consent from contributors.

Action

Ordinarily the personal data that we capture will only be for the purposes stated i.e. for use in one specific production. However, the Production Manager and Production Lawyer should be made aware of when the company would like to use personal data for another purpose in order to agree the basis on which we will notify the contributor of the new use and either the legal ground for processing we are relying on or, if none available, to seek consent for new purpose for which we wish to process the personal data. Minor changes eg to data retention periods can be dealt with via the issuing of an updated production privacy policy.

C) Relevant and limited only to those purposes

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Action

The Production Lawyer should ensure that any request for personal data on contributor release forms and contracts is specifically targeted to what is necessary and is in line with the Production Privacy Policy.

Production Managers should ensure that any request for personal data gathered in the course of production should be specifically targeted to the needs of the production and is in line with the Production Privacy Policy / Data Management Plan.

D) Accurate and Kept Up to Date

Personal data must be accurate and kept up to date. Steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Action

Production Lawyer to include an obligation on contributors / production personnel to provide any necessary updates to their personal data to ensure company records and accurate and up to date. Production Managers should be aware of the requirement to make corrections to information on an ongoing basis.

E) Kept only for as long as is necessary for the purposes the data subject has been told about

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

Action

The production-specific privacy statement should include data retention periods eg name and contact details and signed contract /release forms will need to be kept forever in case need to contact contributor for any legal / regulatory reasons etc and as provide evidence of grant of rights but production-specific personal data eg background checks can be destroyed say 12 months after broadcast with any information which could be linked to a legal claim (eg medical information on a medical show) kept for a period of 7 years from collection.

Ordinarily, information we collect from individuals for a programme will need to be handed over to the commissioning broadcaster and then at a later date to programme distributors/licencees in order to show that the programmes are cleared for exploitation. Therefore the release forms should explain that we will use the data in this way.

F) Kept Securely

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We must put in place procedures and technologies to maintain the security of

all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with GDPR mandatory data processor obligations.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal.** Paper documents should be shredded. Portable memory devices should be deleted when they are no longer required using appropriate IT approved software.
- **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

Action

Ensure that all employees/freelancers and in particular Production Managers follow these Data Protection and Data Security Guidelines.

Liaise with the IT Department on each production to secure assistance and support with ensuring suitable data security measures are implemented for the production.

Ensure that we have contracts with any third party to whom we share personal data and that our template GDPR compliance data controller to data controller or data controller to data processor clause are used (or equivalent provisions).

See below PACT Production Company and PACT Production Crew Data Security Guidance.

In addition we must ensure that personal data is:

G) Processed in line with data subjects' rights

Personal Data must be processed in line with data subjects' rights details of which are set out in the company's Website Privacy Notice. This includes the right to request copies of their own personal data (see section 3, below) and, from 25 May 2018, data subjects will have additional rights to request that:

(a) any inaccurate personal data about them is corrected;

(b) their personal data is deleted;

(c) we stop using their personal information for certain purposes;

(d) personal data is provided to them in a portable format; and

(e) decisions about them are not made by wholly automated means.

Some of the rights listed above are limited to certain defined circumstances and we may not be able to comply with all requests.

Action

Ensure that all employees/freelancers and in particular Production Managers refer to the company's Individual's Rights policy and refer any subject access requests to the Tinopolis Group Data Protection Manager.

H) Not transferred to people or organisations situated outside the EEA without ensuring adequate protection.

Action

Our contributor release forms and employment contracts should state that we may pass on information to foreign territories and we should ensure that our licences and distribution agreements make provision for proper handling of personal data.

Ensure that we have contracts with any third party to whom we share personal data outside of the EEA and that our template GDPR compliance data controller to data controller or data controller to data processor clause are used (or equivalent provisions) and require the third party to provide adequate facilities and equipment to put this into practice.

3. Dealing with "Subject Access Requests"

Any data subject can make a request for information that we hold about them. Any member of staff who receives such a request should forward it to the Tinopolis Group Data Protection Manager **immediately**.

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

- Refer to the Tinopolis Group Data Protection Manager Data Protection Manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

4. What happens in the event of a breach?

If anyone becomes aware of a breach of these guidelines they should **immediately** alert the Tinopolis Group Data Protection Manager who will decide what course of action is appropriate. If the breach relates to programme material e.g. it relates to contributors, contestants or talent the Tinopolis Group Data Protection Manager will liaise with the production team who may need to alert the commissioning broadcaster and the PR department in relation to any press statement that may be necessary.

PACT Data Security – Crew Guidance (2018 GDPR version)

Please see the attached.

Producers' Data Protection and Security Guidelines:
Production Crew – General Notes

These notes set out practical advice and assistance for you when dealing with **living people's personal data (including Special Category Data)** under the General Data Protection Regulation (GDPR) effective as of 25th May 2018.

It's important to protect individuals' data, under the GDPR there can be criminal and civil sanctions for the production company when there is an unauthorised disclosure of Personal Data and Special Category Data, as well as reputational damage for the production company you are working for and potentially for your commissioning broadcaster.

Personal data under the GDPR relates to anyone who can be identified as a living human being from the data or from that data and other readily accessible information e.g. **any one or more of** their name, address, telephone numbers, personal email addresses, date of birth, bank and pay roll details, next of kin, passport particulars, images, IP address etc.

Special Category data (previously known as 'Sensitive Personal Data') requires extra care. It includes information relating to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health matters, sexual orientation, genetic or biometric data, alleged or actual criminal activity and criminal records. Note: Information relating to criminal offences and Children's Data now have their own provisions on how they should be dealt with. You should check with your line manager that all necessary safeguards are in place for handling such data. If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.

Under the GDPR you must have a **lawful basis** for handling any type of personal data. It is important that before you collect any personal data, that you understand and have agreed with your production company, for example by you or nominated personnel as to the lawful basis on which you are processing personal data when you are employed/ engaged by the company and that the lawful basis for processing is documented. For example, when dealing with contributors, your agreement with them will most likely state that the lawful basis for processing is for the performance of a contract or legitimate interests. If you have not been advised by your line manager or are unsure of the lawful basis you are relying on to collect or handle data, you should speak to your line manager or nominated personnel

Here at Tinopolis Limited and its UK group companies, [*insert nominated personnel*] is responsible in the company for complying with the GDPR. You should contact this person if you are unsure of your obligations under the GDPR when collecting, using, processing, accessing and destroying personal data.

Collecting and accessing personal data

You will have access to or routinely acquire personal data and, potentially, special category data in many forms. This information may be from past, current and future employees, contributors, suppliers and contractors.

This information may be in the form of letters, emails, correspondence, call logs, programme treatments, running orders, CV's, CCTV, contributor agreements or release forms, contributor application forms, call sheets, P-as-Cs, disclosure & barring service checks, medical records, invoices, purchase orders, rushes with captions, bank statements, lists of employees or employee references to name a few. The information can be in **hard copy form** e.g. original or copy paper document, photographs and film; or in **electronic form** e.g. held on a PC, laptop, mobile phone, blackberry or memory stick.

What personal data should you collect?

You should **only collect what you need. Under the GDPR this is the personal data that is necessary for the purpose for which you will use it.** For example it may be reasonable to collect the name and contact details of

contributors so you can organise filming with them, but it is very unlikely you would need information regarding their sexual history to carry out that function, unless it was relevant to the programme.

What do you have to tell the person from whom you are requesting the information?

You should tell the person why you need to collect the personal information and what you are using it for, the lawful basis you will be using to process the information, how it will be shared and stored and how long it will be kept and remind them that rights in respect of personal data are protected by the GDPR.

When you communicate this to the individual, it should be in a *clear and concise* manner using language that is easy to understand. If you are collecting and processing personal data that relates to children, you will need to ensure that you provide an explanation in an age appropriate way (if it is not to their parent/guardian), so the child can understand what will happen with their data and consider whether you also need to contact their parent or guardian.

How can you use the information?

You can only use personal data for the purposes for which it was collected or given to you. For example, it may be that the personal data was only provided by a contributor for the purposes of a particular Programme and not for any other use. However if you wish, for example, to contact applicants to a programme in the future to be involved in other programmes or to receive marketing information then you can request their consent to do so. That consent must be specifically and freely given for the relevant purposes, and the individual will have to opt-in to each purpose (you must also set out how they can withdraw consent). Remember, if you use consent, it cannot be made a condition of being involved in a programme and you should also inform the person that this consent can be withdrawn and how to do so. This should be expressly stated on any form that is being issued.

Anonymization

Effective anonymization can be used to publish data which would otherwise be personal data. The ICO defines Anonymization as the process of rendering data into a form which does not identify individuals and where identification is not likely to take place through its combination with other data. A risk assessment should be carried out before such anonymised data is processed. A useful test which can be used is the Motivated Intruder Test.

Anonymization might be used where audience members wish to share their stories or experiences, but the data provided is sensitive. For example, if individuals wanted to contribute to a story about their experiences with the NHS, those contributions might need to be aggregated or anonymised in order to provide support for a story without linking it to a specific individual. Anonymization might also be used where an organisation wishes to share data for research purposes.

http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

Handling personal data

1. Personal data should be kept secure to avoid, loss, damage or unauthorised access. You need to make sure that personal data is not left on your desk when you are not there. It should be stored in a locked office or other secure area. Where appropriate, files containing special category data should be kept locked on or off site. All portable media devices containing personal information should be encrypted using either BitLocker or FileVault.

2. Have you password protected your computer and do you regularly update it? If you use or have access to personal data that could cause harm if lost, stolen or improperly accessed (e.g. financial, records, health information, child related or other special category data) your laptop computer, PC or other device should be password protected and your desktop protected by a secure firewall.

3. Are you providing or restricting access to the information whether on computer or hard copies to only those who are authorised or need to have access to? *Any documents that contains personal data (and few documents don't!) you must ensure that they are electronically stored either (a) in a secure part of the server with the appropriate access limitations or (b) within an encrypted/password protected folder.*

4. Be careful when opening unrecognised emails and attachments or visiting new websites to prevent viruses which may pose risk to data security.

5. Keep your computer screens/notice boards and white boards positioned away from windows/public view to prevent accidental disclosures of personal data.

6. Ensure that visitors or guests to the office cannot view personal data and implement measures to prevent accidental disclosure to them.

7. Do you have permission to take computers, laptops, computer discs etc, off the premises? If so, do check that they have appropriate password protection and for special category data, children's, criminal and financial data, and that there is a high level of encryption for the relevant folder or for the computer/discs etc. as a whole or other effective protection in place? If you have a work mobile which contains contributor's details keep it password locked and coded so that if the equipment was lost or stolen or an attempt to hack into it the personal data be secure. The loss of portable or mobile devices that include magnetic media used to store and transmit personal information could cause serious damage/distress to the individual should it become public. The ICO recommends protecting such devices with approved encryption software designed to safeguard against compromising information.

8. You should advise your line manager if you are taking personal data off site and when you have returned it.

9. Make only as many copies of personal data as are necessary for distribution to those who need it (again just for the purposes for which it was collected) and ensure that those in receipt of the information are aware of the need to and are able to keep the information protected in the manner set out in these guidelines.

10. Make sure that you are aware of which documents should be shredded and/or put in the "security safe" recycling bins/boxes.

11. Take extra care when faxing/sending personal data so that only the intended recipient receives the information. Always use the most secure method of sharing information available.

12. If you receive a request from the police for information you should advise your line manager **immediately** and where appropriate seek prompt advice from your commissioning broadcaster. Where the request relates to programme material including rushes, you should consult with your commissioning broadcaster before making any disclosure as there may be legitimate legal and editorial grounds for resisting disclosure.

13. On close down of a production you should ensure a senior member of staff has reviewed what personal data records can be legitimately retained or destroyed. The production company may need to legitimately retain information for a legal or business purposes, for example there may have been an accident or ongoing litigation where documents must be preserved by law. You should ensure that you have the necessary internal permission when destroying personal data.

14. Have you ensured you have returned and/or destroyed documents, memory sticks and/or DVDs that have been taken off the premises? Where you need to destroy documents have you got relevant permission from your line manager?

15. At the end of your employment with the company have you returned all confidential and/or personal data or if the company agreed for you to do so should delete information from any personal computer or mobile devices you were using.

Security Breach

In the event you become aware of a breach of security or an unauthorised disclosure or loss/theft of documents or information in another form, you should alert your line manager and the senior member of your staff responsible for data protection matters immediately. If the breach relates to programme material e.g. it relates to contributors, contestants or talent your line manger should also alert your commissioning broadcaster as soon you become aware and take any further appropriate action that may be advisable.

You should also take immediate action to find out the extent of the potential harm to the person(s) concerned and take immediate steps to mitigate any harm/ damage to that individual, however please do not contact the individual until you are instructed to do so. Your line manager or nominated personnel will agree the best course of action as to how to inform individuals and, where appropriate, the relevant regulatory authority.

You should be aware that our security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal.** Paper documents should be shredded [shredders are located in stationery area on each floor]. Portable memory devices should be deleted when they are no longer required using appropriate IT approved software.
- **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

Remember: Protect and respect personal data. Don't lose personal data, or let it be stolen, pretend it is your own personal data (or money).

END

Glossary of Terms

Key Definitions:

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Special categories of personal data means information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information for uniquely identifying a person, information concerning health, and information concerning a person's sex life or sexual orientation. Information concerning criminal convictions is placed in a similar category. These special categories are concerned particularly sensitive and we will therefore only process this information where absolutely necessary in accordance with additional safeguards.

Processing is any activity that involves 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. Processing also includes transferring personal data to third parties.

Data subject means, for the purpose of this policy, all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data controller is the organisation which determines the purposes for which, and the manner in which, any personal data is processed. A data controller is responsible for establishing practices and policies in line with the data protection legislation. For example, we are the data controller of personal data used relating to our own staff.

Data processor is any organisation that is not an employee that processes personal data on behalf of and on the instructions of a data controller. For example, we are a data processor where we handle personal data on behalf of a customer.

Read and agreed by: .....

Date: .....