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 Data Protection Act 2018 ('**DPA 2018'**) which implements 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, images, IP address etc.

Special category data (previously known as 'sensitive personal data') is also personal data and is information that 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. This personal data cannot be processed unless you are able to apply Article 9 of the GDPR[1] which sets out the additional conditions for processing special category data. If you are unsure of what special category data you can process, please speak to your line manager. 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 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 [*insert production company name*], [*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, CVs, 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.

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

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.

More information is available at the ICO website:
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. Find out what security is in place by asking a senior member of staff or nominated personnel if you are unsure.

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? You must ensure that *any document that contains personal*

data (and few documents don't!) 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, check that they have appropriate password protection and for special category data, children's, criminal and financial data, check 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 contributors' details keep it password locked and coded so that if the equipment was lost or stolen or there was an attempt made to hack into it the personal data is kept secure. The loss of portable or mobile devices that include magnetic media used to store and transmit personal data 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) you should delete confidential or personal 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. This is due to timescales for reporting breaches to the ICO that are imposed on companies by the GDPR. This means, for example, a production

company might have to report a breach (depending on the type of breach) to the ICO within 72 hours of the company becoming aware of the breach. If the breach relates to programme material e.g. it relates to contributors, contestants or talent your line manager should also alert your commissioning broadcaster as soon you become aware and take any further appropriate action that may be advisable.

ICO's guide on breach reporting - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

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 such as the ICO.

You should be aware that
[*Please complete with useful information relevant to your own **company policy's** or set out your production company's practical advice and support in ensuring personal data is handled securely, e.g. locations of shredders, security safe recycling bins, lockable cupboards, automatic computer backups, provision of password or otherwise secured equipment, IT support plus links to any other relevant company policies, e.g. for use of internet, emails].*

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