



**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 sensitive personal data)** under the Data Protection Act 1998 ('DPA').

It's important to protect individuals' data. Also, under the DPA there can be criminal and civil sanctions for the production company when there is an unauthorised disclosure of personal and sensitive data, as well as reputational damage for the production company you are working for.

**Personal data relates** to anyone who can be identified from the data or from that and other readily identifiable 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, etc.

**Sensitive personal data** requires extra care and except in limited circumstances can usually only be collected, and used **with the express consent** of that person. Such information relates to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health matters, sexual orientation, alleged or actual criminal activity and criminal records.

Here at **[insert production company name]**, **[insert nominated personnel]** is responsible in the Company for complying with the DPA. You should contact this person when you are unsure of your obligations under the DPA 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 sensitive personal 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, correspondence, call logs, programme treatments, running orders, CV's, CCTV, contributor agreements or release forms, contributor application forms, call sheets, P-as-Cs, criminal record bureau and/or disclosure & barring service checks, medical records, invoices, purchase orders, rushes with captions, bank statements, list of employees, and employee references. The information can be in **hard copy form** e.g. original or copy paper document, photographs and film; or in **electronic form** e.g. PC, laptop, mobile phone, blackberry or memory stick.

**What should you collect?**

You should **only collect what you need**, for example it may be reasonable to collect the name and contact details of contributors but it is very unlikely you would need information regarding their sexual history, unless it was relevant to the programme.

**What do you have to tell the person who is giving you the information?**

You should tell the person why you are collecting the information and what you are using it for and how it will be shared, and remind them that they are protected by the DPA.

**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 obtain consent from the person to contact them in the future to be involved in other programmes, or to receive marketing information or to contact them for other opportunities, then you are permitted to do so. This can be expressly agreed when the contributor signs the relevant consent form or at the point they provide their information e.g. in an application form.

## **Anonymisation**

Effective anonymisation can be used to publish data which would otherwise be personal data. The ICO defines Anonymisation 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 published to any group sizes. A useful test which can be used is the Motivated Intruder Test.

Anonymisation 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. Anonymisation 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](http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation)

## **Handling personal data**

1. You need to make sure that personal data is not left lying around on your desk when you are not there unless you work in an office or area that is locked. Where appropriate, files containing personal sensitive data should be locked on or off site. Find out what security is in place with a senior member of staff.
2. Have you password protected your computer and do you regularly update it? Where you have data that could cause harm if lost (eg financial, health, children or other sensitive data) your laptop computer should be encrypted 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? *Where documents contain personal data (and relatively few documents don't!) ensure that they are electronically stored either in a secure part of the server with the appropriate access limitations or within an encrypted/password protected folder.*
4. Are you careful when opening unrecognised emails and attachments or visiting new websites to prevent viruses?
5. Are your computer screens/notice boards and white boards positioned away from windows/public view to prevent accidental disclosures of personal data? Can visitors or guests to the office view the personal data? Have you implemented measures to prevent this happening?
6. Are you monitoring your visitors/guests around other people's personal information to prevent accidental disclosure to them?
7. Do you have permission to take computers, laptops, computer discs etc, off the premises, if so, do they have appropriate password protection and for sensitive, children's and financial data, is there a high level of encryption for the relevant folder or for the computer/discs etc. as a whole or other protection in place? Where you have a work mobile which contains contributor's details can it be password locked and coded? If the equipment was stolen would 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 sensitive information become public. The ICO recommends protecting such devices with approved encryption software designed to safeguard against compromising information
8. Have you advised your line manager that you are taking the data off site and when you have returned it?
9. You should only make as many copies as are necessary for distribution and ensure that others in receipt of the information are aware of the need to keep the information protected.
10. Are you aware and do you know what documents should be shredded and/or put in the "security safe" recycling bins/boxes?

11. Are you taking care when faxing sensitive personal data so that only the intended recipient receives the information? Is there a more secure method of sharing information?
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 has a senior member of staff reviewed what personal data records can be legitimately retained or destroyed? There may be reasons outside of the production that might require the production company to legitimately retain information for legal or business purpose, 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 information.
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 deleted the information from any personal computer, mobile or blackberry equipment you were using?

Here at [insert production company name] you should be aware that [Please complete with useful information relevant to your own 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 back ups, provision of password or otherwise secured equipment, IT support plus links to any other relevant company policies, e.g. for use of internet, emails]

**In the event you become aware of a breach of security or an unauthorised disclosure or loss/theft of documents, 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 manager should also alert your commissioning broadcaster and take any further appropriate action that may be advisable.**

You should also take immediate action to identify the potential harm to the person(s) concerned and take immediate steps to mitigate any harm/ damage to that individual.

**Remember:**

**Protect and Respect Personal Data. Don't lose personal data or let it get stolen – pretend it is your own personal data (or money).**

**END**