BBC

Information Policy & Compliance

Children's Privacy Guidelines
-
Working with Children
& the BBC

February 2009-02-18
Version 1.4

1. Introduction

These guidelines form the basis of the working practices that the BBC would expect to see as the minimum standards for any independent production company working with children on a BBC commissioned programme or series. They are not designed as a definitive list. If further issues arise, they should be raised initially with the BBC Executive Producer, who may then involve the Information Policy and Compliance Department (IPC)

It is formed of two sections: the IPC guidelines on dealing with children's data; and the Children's and Young Persons' policy section of the BBC's data protection handbook.

2. Guidelines on Dealing with Children's Data.

These guidelines apply when any production is processing children's data.

- The production company will have an up to date and adequate data protection policy, which will deal specifically with the problems associated with collecting data in a programme making environment.
- All staff who work on the programme will be made aware of their responsibilities under the Data Protection Act 1998 (DPA) and be given a copy of the production company's data protection policy.
- One senior member of staff on the production will be given specific responsibility for ensuring data protection guidelines are observed on the programme. The BBC will be informed of their name before production commences and the relevant details will be set out in Schedule 2 of the Commissioning Specification.
- The producer will securely store all personal data relating to subjects, potential subjects, their friends or relations or any contributors to the programme.
- Where hard copy documents are required these will be kept in a secure locked cabinet or equivalent, with access only provided to staff with a specific need for that data.
- Any data stored electronically will be kept on a secure server or PC with firewall protection and any additional security as required by your own data protection and/or information security policy and, at the least, in line with generally accepted current industry standards. For further information may be seen at the Information Commissioner's Office website. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security%20v%201.0_plain_english_website_version1.pdf
- Access to children's data will be limited to those staff with a specific business need to access it.
- If it is necessary to take any data away from the production company's offices, it should be securely transmitted and/or stored. If it is being transported on any portable media such as a laptop, USB memory stick, CD, etc. it should be encrypted.
- Consideration should be given to data security generally. The independent production company may wish to circulate the BBC Information Security top tips (attached as an appendix to this document) or their own equivalent.
- Consideration should be given to giving data protection training to all staff working on the production

3. Children's and Young People's Personal Data – Policy Section of the BBC's data protection handbook

(N.B. The numbers from this point in these guidelines refer to the chapter sections in the BBC's Data Protection Handbook.)

As well as our strong commitment to all users, the BBC is fully committed to ensuring that children's personal data never falls into the wrong hands.
This module sets out the procedures the BBC must follow to ensure that there are safe places for children to visit on the web and to allow them to interact with their favourite programmes and characters.

Note that a "parent" is either a "parent" or a legal guardian.

Children are data subjects under the Data Protection Act and therefore they attract the same protection under the act. However, in order for the child to be bound by the terms of a website or a competition and also to safeguard their interests (for example when making a content contribution), children under 16 will have to have parental consent to supply their data to the BBC. If the child is old enough and it is feasible and appropriate the child's consent should be sought as well as the parents.

5.1 Consent – What is appropriate at what age?

The following sets out how to decide which form of consent is appropriate for the project and audience you are working with:
Verifiable parental consent

The form of this consent will vary according to the age of the child and the level of interaction we are having with them. It can be that with older children and low levels of interaction a check box completed by the child, in other circumstances it will be appropriate to demand a verifiable parental consent, such as signed consent form or a recorded telephone conversation with the parent.
Consent methods:

- Tick box online completed by the child
- Tick box on-line completed by the parent
- Form to be printed by the parent, signed and returned by mail
- Email consent (from a different email address from the child)
- Telephone conversation with the parent (contemporaneous notes taken and stored)
- Face to face meeting with parent
- Consent form signed and verified

5.2 How do I decide what sort of consent is appropriate?

Ages of children (different considerations)

Under 12
Under 12's will always need parental consent before supplying any personal data to the BBC. The style of that parental consent be related to the level of interaction as well as their age, but a record of the parental consent of whatever form will be needed.
Where we are asking for children's personal details online it is important to ensure that the reasons for needing the data are explained and a fair collection notice understandable by

children of the age of the target audience is in place. In an online environment the need to ensure consent is particularly important, as there are specific guidelines are in place which the BBC needs to observe.
For contributions to programmes current Editorial Policy guidelines should be adhered to. In certain circumstances the need for parental consent may be waived - for example a vox pops on an uncontroversial subject from 11 year olds.

12 – 16
In this age range it is to be expected that the level of competence will increase. Therefore the older the young person, the more likely that we can accept low levels of personal data without parental consent. There is a difference however between the consents needed to allow us to collect data required by us to provide a service or that which we will publish. For example an email address to send a newsletter to, might only need a tick box consent, whilst a video on a website, would normally need stronger verification.
Any broadcasting/publication in this age range should be pre-moderated, whether of photos, video or messages, etc.

16 – 18
The BBC does not require parental consent for young people in this age range supplying us with personal data as they are deemed by us to be capable of providing fully informed and specific consent where request.

5.3 Assessing risk – levels of interaction

BBC Children's has traditionally classified interaction with children in one of four levels: Very Low level; Low level; Medium Level; and High level. In terms of data protection this might be seen as:

Very Low Level: an interaction but without the collection of any personal data, e.g. SSO registration using a nickname and a password but no email address.
Low Level: Minimal amounts of personal data collected for internal purposes only, e.g. collection of an email address purely for the delivery of a newsletter containing no marketing information.
Medium level: The collection of personal data and the publication of some of the data, e.g. publication online of a winning entry with a first name and large town.
High Level: the publication of some personal data on a BBC service, e.g. A Blue Peter competition where first name, location (large town) and artwork of a winner(s) is published on the website and or the winner(s) are invited onto the show.
This level of interaction will need to be combined with the age of the child to decide whether parental consent is required and what is the appropriate level of verification required.

5.4 Storage and security of children's data

Children's data should always be stored in the most secure way possible in the circumstances including as follows:

- Only those people with a genuine business need to see the data should be allowed access (they will need to be CRB checked, see below).

- The data should always be password protected, with the password being changed regularly and whenever there are staff changes.

- If the data is to be stored on a network server the technical staff with access to the server will also need to be CRB checked and other security processes put in place (contact BBC Information Security for further details).

If you are processing children's sensitive personal data further measures may be needed and you must contact IPC for advice.

5.5 Security of Staff dealing with Children's Personal Data

All staff who will have access to children's personal data will need to have a Criminal Records Bureau check. See the CBBC Connecting with Audiences document for more details of security requirements for working with children.

5.6 Children's data and retention Schedules

All departments should adhere to the same retention periods for Children's data.
If you are not sure of how long you should keep children's data please contact IPC or your Data Protection representative.

Unless correspondence is ongoing, is a complaint or a competition winner, it should be disposed of after one month. For example general comments about a show (that have no archival value) would not be considered ongoing.

For generic mailboxes, empty the deletion box for incoming items at least once a month and the sent items after retaining for one year.

Competition winners' and non-winners' details should be kept for six months, except for premium rate telephony competitions and online competitions. Non-winner details are kept for this period in case the programme is audited regarding the skill level of the competition. Premium rate telephony competition entrants' and online competition details should be kept for two years in case there are any complaints or queries following the competition and to facilitate audits.

As a general rule, contributor details, CV's and emails should be kept for a maximum of two years, if you are retaining them solely for the possibility of future use. You must get express consent to do this on your consent form and you need to provide some way, (e.g. an email address) for individuals to notify of any changes to their details

Rushes, DVDs and VHS' containing footage of children should be erased asap if not used in final programme or 6 months after first transmission.

Information security at the BBC is EVERYONE'S responsibility.

If you have any questions about how best to keep confidential and personal information safe - please contact Information Security at ism@bbc.co.uk.

Please see below a quick reminder list of some easy steps to take keep information secure.

- Don't click on any links in mails from people you don't know. Always take great care clicking on anything in a e-mail, even if you do know them.
- Clear desk policy - leave nothing on your desk that contains any personal or confidential data
- Ensure you lock your computer when you leave your desk using a password protected screensaver
- Don't EVER write your password on post-it notes or anywhere that people may find them
- Lock cabinets. Every night. And during the day when you're not using them.
- Don't give your passwords to anyone
- Lock confidential waste away overnight
- Shred sensitive data by hand
- Never leave visitors alone
- Challenge people not wearing passes - if you feel it is safe and appropriate to do so; otherwise please report the incident to site security
- Keep distribution lists up to date - remove expired persons ASAP
- Only send emails to necessary people
- Blind copy where possible, especially for big distribution emails.
- Don't have confidential conversations in public places, including BBC lifts, canteens, etc. (I know it sounds obvious, but you'd be amazed what you hear...)
- Always check entire email chain for data to ensure you're not inadvertently sending inappropriate info to too many people
- Check the print queue is actually going to the printer you think it is (send a test page or doc first)
- Use private print job function for sensitive data Only print when absolutely necessary (and great for the environment too!) Phone Service desk for instructions if you don't know how to do this
- Be very careful about portable devices - do you need to take data outside of the BBC? Are there any processes you need to follow to do this?
- Always think twice before doing any work (reading or writing paper as well as using a laptop) in a public place -- train, bus, pub, etc.
- Keep your voice down if you have to talk about work or make phone calls in public places.
- Apply both physical and logical security if ever you work from home - keep work items (CDs, DVDs, memory sticks, etc.) secured as you would at the office - and out of reach of anyone else.