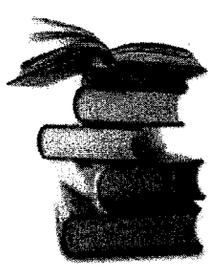
BBC

DATA PROTECTION HANDBOOK

June 2009



BBC Data Protection Handbook

Welcome to the BBC Data Protection Handbook, which sets out the BBC's approach to Data Protection and offers guidance and information about DP within the BBC.

Contents

Module 1 - Introduction

1.1 What is data protection law?

Data protection law gives people the right to control how their 'personal information' (any information that relates to them, such as a name, contact details, preferences etc) is used. Organisations such as the BBC that use personal information are under obligations to use such information responsibly.

1.2 Why is data protection important?

Data protection is about protecting people's privacy. This includes all people who are connected with the BBC in some way - employees, contractors, contributors, website users etc.

1.3 Why is it important to get it right?

The BBC is committed to protecting the personal information of audiences, employees and contributors in accordance with the law.

It's therefore important that the BBC gets data protection right because:

- It affects everyone involved with the BBC; and
- It's key to the BBC's role as a public service broadcaster that it follows the rules on data protection, which need to be carefully balanced with the BBC's freedom of expression in its programme making.

It is in your interests as a BBC employee or contractor to ensure that you protect the personal information you use as if it were your own. Failure by BBC Staff to observe the rules in this Data Protection Handbook (the "Handbook") is cause for disciplinary action which could involve dismissal.

1.4 What records are covered?

Anything which includes personal information (i.e. both hard copy and electronic records) must be used in accordance with this Handbook.

1.5 Who is affected?

Everyone at the BBC is accountable for following and upholding the requirements of this Handbook. If, as a BBC Staff member, you collect any details about individuals in the course of your work, you will be using personal information. This means that you must abide by the rules set out in this Handbook. This Handbook sets out all the tools you're likely to need relating to personal information in your day to day work.

1.6 Who can help within the BBC?

The Information Policy and Compliance department within the BBC is responsible for overseeing the BBC's compliance with the BBC's obligations under the DPA and the Freedom of Information Act 2000 (FOIA).

To find out the IPC Adviser for your division, check the IPC Gateway site.

Module 2 - Overview of Data Protection

The Data Protection Act 1998 (DPA) protects individuals' privacy by regulating how personal information (defined in the DPA as '*personal data*') is collected, used, disclosed and stored.

2.1 The Rules

In order to comply with the DPA, the BBC must follow rules about how personal information is used:

1. We must ensure that there is a lawful ground for using the personal information;
2. We must ensure that the use of the information is fair and that we meet one of the specified conditions.
3. We must only use sensitive personal information if it is absolutely necessary for us to use it.
4. We must only use sensitive personal information where we have obtained the individual's express consent, unless an exception applies.
5. We must explain to individuals, at the time their personal information is collected, how that information will be used by the BBC.
6. We must only obtain and use personal information for those purposes which are known to the individual.
7. We can only change the purpose for which personal information is used if we make people aware of such a change and they can express their concerns.
8. We must only keep personal information that is really relevant to us.
9. We must keep personal information accurate and up to date.
10. We must only keep personal information for as long as is really necessary.
11. We must always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal information.
12. We must always adhere to our Information Security Policies.
13. We must ensure that providers of services to us also adopt appropriate and equivalent security measures.
14. We must never transfer personal information to suppliers or partner organisations outside the BBC without ensuring that they provide the right level of protection.
15. We must always allow individuals to opt-out of receiving marketing information.
16. We must always suppress the details of individuals who have opted out of receiving marketing information.

Throughout this Handbook these rules are repeated where they are relevant to the work at the BBC.

It is important to understand the reasons behind each rule and the practical steps to follow in order to comply with the rules.

Rule 1: We must ensure that there is a lawful ground for using personal information

Understanding the Rule

This is part of the principle in the DPA to only use personal information fairly and lawfully. The BBC must always be able to rely on a lawful ground to use personal information e.g. the BBC is required to pass on details about employment and salary terms to HM Revenue and Customs for taxation purposes. Although the BBC is also required to inform individuals about how the BBC will use their personal information, we can never use personal information in a manner that is unlawful. For example, obtaining personal data about an individual by impersonating them is a criminal offence (this practice is known as "blagging" and the regulator is seeking increased penalties for those convicted of it).

Practical steps

We need to be sure that what we want to do with the personal information is lawful. Ask yourself whether the purpose for using the information might be contrary to any law. It may be obvious that a purpose is lawful, such as where the BBC is required to use the information in order to comply with its own lawful obligations. If in doubt, please contact the IPC Team.

Rule 2: We must ensure that the use of the information is fair and that we meet one of the specified conditions

Understanding the Rule

The BBC must use personal information fairly. To ensure that the use is fair, the BBC must consider the consequences of the proposed use to the interests of the individual. If there is a concern that the use may be detrimental to the individual, then the use may not be fair. As a guide the BBC should consider whether the use of the personal information would be within their reasonable expectations.

Practical Steps

Additionally, to use personal information the BBC must always meet one of the specified conditions. One of the specified conditions is the consent of the individual concerned and it may be fair to assume implied consent in certain circumstances (e.g. where an individual writes to the BBC they implicitly consent to their personal data being processed to deal with their query). Furthermore, in many cases it will be possible to rely on the specified condition relating to the legitimate interests of the BBC in using the personal information so long as there is no prejudice to the individual concerned. However, when using sensitive personal information (e.g. information about someone's health or religious beliefs), the BBC needs to meet an additional condition. Please see Rule 3 and Rule 4 for further guidance on sensitive personal information.

Please contact the IPC Team if you are not sure which condition to apply.

Rule 3: We must only use sensitive personal information if it is absolutely necessary for us to use it

Understanding the Rule

Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. This information deserves even stronger protection than other personal information, so our standards of care must be higher when dealing with this type of information.

Practical Steps

You should always assess whether sensitive personal information is essential for the proposed use. If you can achieve your aim without using sensitive personal information, then do not use it. Please remember the greater expectation of privacy that people attach to these pieces of information.

Rule 4: We must only use sensitive personal information where we have obtained the individual's express consent, unless an exception applies

Understanding the Rule

Given the nature of this type of information, it is usually only appropriate for us to collect and use it when people agree. This permission to our use of sensitive personal information must be genuine and freely given.

Practical Steps

When you use a form to collect sensitive personal information, it must include suitable wording explaining to the individual why this information needs to be collected and that the individual is giving explicit consent for this purpose.

Consent must be demonstrable. When you collect it verbally it must be recorded in such a form as to prove that the requisite information was provided to the individual and their response is capable of being verified.

Where consent is not possible, you should contact the IPC Team to consider whether an exception applies.

Note on financial information: Financial personal information is not defined as "sensitive personal data" under the Act, but nonetheless deserves special protection due to the serious harm that can result from its misuse.

Rule 5: We must explain to individuals, at the time their personal information is collected, how that information will be used by the BBC.

Understanding the Rule

The BBC must provide certain information to notify the individual about the use of their personal information. Being open and transparent in the way that we use and share our employees' and users' personal information is the single most important step we can take to create good data protection practices within the BBC. This means that individuals are always told in a clear and comprehensive way about the uses, disclosures and processing activities performed on their information when such information is obtained. This is usually done through a Privacy Notice.

Practical Steps

In the context of employees' information, Privacy Notices need to be issued to all employees operating in the EU and where obliged to by law in countries elsewhere.

For users' information, the BBC must make available versions of the Privacy Notice at the points where personal information is collected which will typically include application forms and websites.

The BBC's Privacy Policy is an online Privacy Notice which meets our obligation to use information fairly since it provides website users with information about how we use their personal information when we collect it online. It is important that we also provide specific details at each point where we collect information.

You must also ensure that if you make changes to the personal information you collect via the bbc.co.uk website, or you change the purposes for collecting personal information, your activities are consistent with your Privacy Notice and the BBC Privacy Policy.

See the section **"What must we tell people when we're collecting information about them"** for examples of Privacy Notices.

KEY QUESTIONS

- Are those you hold, or collect personal information about clear as to what you are collecting and how it will be used?
- Does your use of the information satisfy one of the conditions set out in Rule 2?
- Do you have explicit consent to process sensitive personal information? Could you provide evidence of this if necessary?
- Is this also the case if you collect data about someone from a third party?

Rule 6: We must only obtain and use personal information for those purposes which are known to the individual.

Understanding the Rule

This rule means that the BBC must identify and communicate the purposes for which personal information will be used (including secondary uses and disclosures of the information) to the individual.

Along with the rules above, this rule limits the use of personal information to the purpose(s) for which it was obtained.

Practical Steps

It is possible to use personal information collected for several different purposes. When collecting personal information from individuals, BBC Staff should consider all likely future uses and communicate these clearly to the individual at that time. But putting a broad 'catch-all' such as "and any other" use in the Privacy Notice is not acceptable. The purpose for using the personal information has to be reasonably clear when the information is collected.

Where BBC Staff would like to involve individuals in a future survey, ask the individuals whether they wish in the first place to be contacted about the survey.

Rule 7: We can only change the purpose for which personal information is used if we make people aware of such a change and they can express their concerns

Understanding the Rule

If personal information is collected by the BBC for a specific purpose (as communicated to the individual via the relevant Privacy Notice or Privacy Policy) and subsequently the BBC wishes to use the information for a different or new purpose, the BBC must ensure that the relevant individuals are aware of such a change. In certain circumstances, the individual's consent to the new uses or disclosures will be necessary.

This means it is important to ensure that when personal information is collected, individuals are informed of all likely uses of that information, in order to minimise the likelihood of having to inform them at a later stage.

Practical Steps

In every case, the individual must be informed of the fact that his/ her information will now be used in a different way.

If the change is likely to be within the reasonable expectation of the individual, then the change can be implemented without obtaining consent.

However if a new use of someone's personal information is likely to have an adverse impact on that individual's privacy rights, the BBC must seek and obtain the consent of the individual before using the information for that new purpose.

There are certain exceptions to this rule. Please contact the IPC Team for further information.

KEY QUESTIONS

- Have you identified all the purposes for which you intend to use the personal information?
- If you have already collected the information, does the new purpose differ from when the information was originally collected? If so, please obtain advice from the IPC Team before proceeding.

Rule 8: We must only keep personal information that is really relevant to us.

Understanding the Rule

Personal information should only be collected where it is relevant. The BBC must identify the minimum amount of personal information that is required in order to fulfil the identified purpose.

This rule is specifically aimed at ensuring that the correct amount of information about individuals is used. In particular, the BBC should only collect or hold the minimum necessary information about an individual in order to carry out the activity.

Practical Steps

This rule applies even if the provision of certain additional information is voluntary. For example, you should not ask for someone's date of birth if all you need to know is their age - simply ask them to state their age or to select the appropriate range from a list of age ranges. If you are interested in knowing what region the individual is from, you do not need to ask for their whole postcode. You could just ask for broader regions ("Yorkshire" or "South-east") or the first part of the postcode.

When collecting information via forms (whether on-line or off-line), the forms should be designed so that only the necessary amount of information is collected.

Furthermore you should consider whether the information you are collecting can be collected on an anonymous basis, in which case it is likely you will not be collecting 'personal information' because you cannot identify particular individuals. Audience research projects are an example of where anonymous information is often used, and hence more questions can be asked about the demographic of the participants without having to identify them. However, depending upon what particular information you are collecting, you should be aware that simply omitting to collect names may not be enough to make the information truly anonymous. If you want to collect anonymous information please contact the IPC Team.

KEY QUESTIONS

- Establish what personal information you really need to collect and why. Do not collect information just because it might be useful to you in the future - it has to be relevant to the purposes for which you are collecting the information now.
- Check the information you are collecting and the design of your forms and telephone scripts against this purpose.
- Stop collecting information or delete information which is no longer relevant or could be considered excessive, even if initially collected on a voluntary basis.
- Consider keeping anonymised information if you don't need to identify specific individuals (for advice please contact the IPC Team).

Rule 9: We must keep personal information accurate and up to date

Understanding the Rule

Inaccurate information can be harmful to the BBC because the BBC will be making business decisions on the basis of out of date or false information. The main way of ensuring that personal information is kept accurate and up to date is by actively encouraging employees and users to inform the BBC when their personal information changes. Where information has been collected directly from an individual or a reputable third party, it is reasonable to assume it is accurate. However, remember that the onus is on the BBC to satisfy itself this is so.

Think about the likely damage or distress which could be caused to an individual as a result of inaccuracy and update the information accordingly. Imagine a local authority that did not update the records of a mother whose child had died. Great distress would be caused to her if the local authority continued to send her information about the child's education etc.

Practical Steps

In the employment context, employees must be actively encouraged to update their details (e.g. change of address), by means of systematic reminders.

All users must be actively encouraged to update their contact details by inviting them to notify the BBC of any changes in their personal information when the BBC communicates with them.

Where information is found to be inaccurate, it should be corrected. If you are not certain about the accuracy of the information, then you should make a record stating that you are not certain, for example in a notes field. This will be sufficient to meet the requirements of this Rule.

In deciding whether you need to update information, you should also take note of Rule 10 below which states that personal information should only be held for as long as is necessary.

KEY ACTIONS

Establish methods to:

- Check the accuracy of personal information when you collect it;
- determine which personal information is actively used;
- keep 'live' personal information up to date; and
- provide and promote mechanisms for users to update their own personal information
- correct, or mark any record which is disputed.

Rule 10: We must keep personal information only for as long as is really necessary

Understanding the Rule

Personal information should only be kept where there is a business or legal need to do so.

For example, statutes or regulations may require that certain personal information be retained for a specified length of time. It may also be prudent to keep certain personal information for a specific period so that the BBC is able to defend properly any legal claims or manage an ongoing business relationship.

Documents (including paper, electronic versions and email) containing personal information must not be kept indefinitely and should always be deleted and destroyed once they have become obsolete or when that personal information is no longer required. Personal information should not be retained simply on the basis that it might come in useful one day without any clear view of when or why.

There must always be a reason why the BBC retains personal information. You need to be able to show that personal information is being held for a purpose. If you can justify the reason for retention you will be compliant with the Act.

If a sufficient reason cannot be shown (just in case the information may come in useful some day does not amount to a purpose) then this Rule imposes an obligation upon the BBC to get rid of the information, or of those parts of the information which are no longer needed. Please see Module 9 - Security and Deletion of Personal Data for more information on this.

Practical Steps

The DPA does not impose particular retention periods. When considering appropriate periods for the retention of personal information, bear in mind that different periods may apply to different personal information which is held for various purposes. For certain records, the BBC's Corporate Retention Schedule will apply.

If you need to keep personal information for the period of a programme series, consider if you can delete it after the series. If you need it for the next series, that is ok, so long as you have truly considered the need to retain the information and can justify retention.

If you are considering keeping personal information for a long time, for example in a personal contacts list, you should consider whether the person knows or reasonably expects you to keep it. If there is no expectation, then you should delete this information. Alternatively, you may be able to anonymise the information if you no longer have a need to identify specific individuals.

KEY QUESTIONS

- Review why you are keeping the personal information.
- Is the purpose for which you first collected the information still relevant?
- Can personal information that you no longer need be deleted?
- Do you have procedures in place to ensure data that is no longer needed is deleted?

Rule 11: We must always adhere to our Access Request Response Procedure set out in Module 15 and be receptive to any queries, requests or complaints made by individuals in connection with their personal information.

Understanding the Rule

One of the most important of all data protection rights is the 'right of access', through which individuals are entitled (by making a written request to the BBC) to be supplied with a copy of any personal information held about them (including both electronic and paper records).

Individuals also have the right:

- To prevent processing likely to cause substantial damage or distress;
- To prevent processing for direct marketing purposes; and
- To have data corrected, blocked, deleted or destroyed if inaccurate, or if damage has been caused.
- To be notified of any automated decision taking (and the rationale used in solely automated decisions)

Practical Steps

If you receive a request from an individual asking for a copy of their personal information, you must follow the procedure in Module 14 - Subject Access Requests.

If you receive a request from an individual to stop using their personal information because it is causing them distress or damage, then please do not enter into discussions with the individual without first contacting the IPC Team and Programme Legal Advice. Please see Module 16 - Complaints for further information.

If you receive a request from an individual to stop using their personal details to send them marketing information, then you must ensure that you stop sending them marketing. Please see Module 11 - Marketing for more information or contact the IPC Team.

In some cases, an individual's data may be processed and a decision which would affect them may be made automatically on the basis of that information. Examples might include where an online psychometric test has to be completed and a minimum score achieved as a condition for applying for a role, or where an individual applies for tickets to an event online and the decision not to allocate them tickets is taken automatically. If you receive a request from an individual about what their rights in relation to automated decision taking please contact the IPC Team.

An individual who obtains a copy of his/ her personal information under a subject access request, may consider that the information is inaccurate and needs to be changed, deleted or destroyed. The individual may request the BBC to change, delete or destroy the information. Where the BBC disputes the individual's arguments, the individual is permitted to take the matter before a court. Please see Module 16 - Complaints for more information or contact the IPC Team.

KEY ACTIONS

- Make sure you and your staff know how to recognise a subject access request (a request from an individual for a copy of their personal information) and forward it to the IPC Team immediately.
- Review all the ways you may be using personal information for direct marketing.
- Make sure individuals have the opportunity to opt out of direct marketing activities,

particularly where personal information is collected online.

- Look at the Privacy notice you provide to individuals at the point you collect their details. If you pass their details onto third parties, is this clearly explained? (The right to object to/opt out of mailings applies equally in relation to third parties.)

- Make sure your databases include the ability to mark those who opt out of direct marketing. Keep this database up to date. Amend or delete records of those notified as 'unsubscribed', 'deceased' or 'moved away'.

- Remember that data which you hold, including emails and hand written notes (e.g. of a disciplinary hearing) may be subject to disclosure - ensure that your communications are always professional and work on the assumption they may be disclosed.

- Remember that once a record is created it may have to be disclosed - don't keep emails longer than necessary and use non-written communications where appropriate.

Rule 12: We must adhere to our Information Security policies.

Understanding the Rule

Personal information must be kept secure. Technical and organisational security methods are necessary to prevent the unauthorised or unlawful processing or disclosure of personal information, and the accidental loss, destruction of, or damage to personal information.

When considering what level of security is required in each particular case, the following factors must be taken into account:

- The state of technological development;
- The cost of implementing any measures;
- The harm that might result from a breach of security;
- The nature of the information to be protected.

The DPA requires the BBC to adopt a risk based approach to the security of personal information held by the BBC.

Practical Steps

Examples of technical measures include the use of passwords, encryption, firewalls or anti-virus software. You should use increased security features according to the sensitivity of the information and the manner in which it is stored (for example, if dealing with children's information or credit card numbers).

Examples of organisational measures include taking steps to ensure the reliability of staff who use personal information, for example through training, and having in place a comprehensive security policy.

We are all responsible for ensuring that personal information is only accessible by those authorised to have it and to that end, must take a number of steps to safeguard this. For example:

- password protect the files;
- use an approved password protected screensaver if you leave your machine unattended;
- do not leave files or printouts lying around where they may be seen by unauthorised people; and
- dispose of waste paper which includes personal information by shredding.
- escort visitors while inside the building
- if transferring personal information use an appropriately secure method of transfer and if in doubt consult the IPC or the BBC Information Security Department via email: ism@bbc.co.uk

BBC Staff must ensure the security of personal information held manually on CDs, USB sticks or on the C: drive. This will normally involve locking the CD or USB stick away at night. Sensitive information must be secure each time you leave your desk and laptops should be locked away when not in use. If you are storing personal information on a memory stick it must be encrypted. You should never dispose of personal information without shredding it. Please be aware that a number of high street banks who disposed of client details in refuse bins without shredding have been publicly reprimanded by the Information Commissioner. We do not wish this to happen to the BBC. Click here for some Top Tips for Information Security.

Rule 13: We must ensure that providers of services to us also adopt appropriate and equivalent security measures

Understanding the Rule

The law expressly requires that where a provider of services to the BBC has access to BBC employees or users personal information, the BBC imposes strict contractual obligations dealing with the security of that information.

Practical Steps

All contracts with providers of services must include the standard contractual provisions made available by the IPC or Regulatory Legal Department from time to time.

Where the BBC uses an agent or contractor, for example an indie producer, to use the information on the BBC's behalf, the BBC is still legally responsible for how that information is used. Consequentially, the BBC must be satisfied with the third party's security measures. Further, a written contract must be in place requiring the third party to process the information solely in accordance with the BBC's instructions and to provide an appropriate level of security for the information. Each time the BBC is considering engaging a new contractor that will use BBC Staff or user personal information, please advise your division's DP Representative and BBC Information Security (the department which approves the technical security of systems and the security policies of other organisations that we work with).

The basic elements you should consider for information security are listed in the Top Tips for Information Security.

It's important to remember that whenever you use BBC information you must comply with the Acceptable Use Policy.

KEY QUESTIONS

- If you are setting up a new database, have you considered where it will be stored and

MOD100018209

how you will limit access to it?

- Are you collecting sensitive information, children's information or bank details? Is the security around this information adequate enough?
- Are you engaging another organisation (a data processor) to collect and store personal information on the BBC's behalf? Do you have a contract in place with them? Have you contacted your DP Representative to obtain their advice?

Rule 14: We must never transfer personal information outside the BBC without ensuring that the third parties provide the right level of protection

Understanding the rule

We can transfer personal information to service providers based in the European Economic Area so long as we comply with Rule 13. The European Economic Area (EEA) consists of the 25 EU member states together with Iceland, Liechtenstein and Norway.

However, there are different rules when the BBC:

- Transfers personal information to service providers based outside the EEA; or
- Transfers personal information to third parties (who are not service providers) based inside or outside the EEA.

The general rule is that personal information should never be transferred outside the EEA unless the information is adequately protected.

The BBC takes the view that transfers within the BBC, from the UK to another part of the BBC outside the EEA, are acceptable provided that all BBC staff are required to comply with the rules specified in this Handbook. For other transfers, including where a third party is involved eg a BBC outsourced supplier or where the data is being transferred from outside the UK, please refer to IPC for further advice.

What is a transfer?

A transfer takes place when personal information collected in the EEA is transferred to a country outside the EEA where the personal information is used. Mere transit, such as where personal information is routed through a third country e.g. the USA, on the way from the UK to another EEA country, is not regarded as a "transfer". However where data can be accessed from a non-EEA country, even if it is physically held in the UK, this is likely to constitute a transfer.

Examples of transfers to a third country include:

- Where a website is hosted on servers in the USA. If the personal information of people in the UK is collected then their information will be "transferred" to the USA.
- Steria processes a great deal of BBC's finance details which can include personal information (such as expenses). Steria has processing operations in India. Therefore this is a transfer of personal information.
- Publishing personal information on a public website is equivalent to allowing the transfer of information worldwide.

Obtaining approval for a transfer

If the arrangement you are entering into means that personal information will be transferred outside the EEA please speak to the IPC Team since this is a complex area. For example, there are certain exemptions available from the restriction on transferring information. Where a BBC supplier may process personal data outside the EEA this will require a) appropriate checks into the supplier's policies and procedures and ability to protect the data overseas and b) specific contractual obligations to be placed on the supplier to ensure adequate protection of the data.

If a third party is being used to host a website, you must comply with the Third Party Hosting Guidelines, and ensure that the third party completes the Information Security hosting questionnaire both of which can be found here

KEY QUESTIONS

- Are you transferring personal information outside the EEA?
- If you are using an external service provider, are all their operations and handling of the personal information based in the EEA, or will they potentially be transferring information outside of the UK? Where are their web servers based?
- If you are transferring personal information outside of EEA have you taken advice from IPC?

Rule 15: We must always ensure that we have received a proper opt-in from individuals who wish to receive marketing before sending them marketing

Understanding the rule

One of the key data protection rights that individuals have is the right to object to the use of their personal information for direct marketing purposes and the BBC must ensure that it receives proper opt-in requests in order to market to individuals and provides individuals with mechanisms to opt-out at a later date should they wish to.

Practical steps

The BBC must ensure that the data protection statement made available when personal information is collected explains to individuals the consequences of opting-in to receive marketing communications.

Rule 16: We must always suppress the details of individuals who have opted out of receiving marketing information

Understanding the rule

It is essential that individual's choices are accurately identified when direct marketing campaigns are carried out. A failure to comply with an individual's opt-out choice (e.g. by

MOD100018210

sending a mailing to an individual who has previously indicated to the BBC that he or she does not wish to receive mailings) is likely to lead to complaints from the individual and possible scrutiny or enforcement action being taken by the Information Commissioner.

Practical steps

Where you are responsible for a direct marketing campaign, you must take all necessary steps to prevent the sending of marketing messages to individuals who have opted out.

2.2 The General Exemptions

There are a number of exemptions contained in the DPA which provide the BBC with exemptions from the Rules in certain situations. Please contact your DP Representative or the IPC Team for further information about exemption.

Module 3 - Contacting the Audience

SUMMARY

If you want to contact the audience remember you must:

- obtain their consent to send them marketing information
- only collect the minimum information necessary
- allow them the ability to opt out of receiving marketing information
- provide a Privacy Notice
- not share the information with third parties unless the individual has consented to this and you have provided details in the Privacy Notice

Data protection rules govern the way that the BBC contacts the audience since the BBC uses email addresses, mobile phone numbers, addresses and names to contact people. The Privacy & Electronic Communications Regulations also impose further requirements in the area of marketing which you may need to adhere to. People trust the BBC to use their personal information properly and responsibly and we must not send them unwanted communications therefore please contact the IPC Team for advice if required.

3.1 Sending Newsletters, e-newsletters and texts

Email newsletters and text alerts can be great ways to keep the audience up to date with BBC programmes and other output. When you want to send a newsletter about BBC programmes and services to our audience members you need to ensure the following:

- They must positively consent to receiving the email or text
- You must only collect the minimum information needed from each individual - e.g. just their email address or phone number if that's all we need. There are special considerations for Children's data - see Module 5 for more information.
- If you wish to send them information about other related BBC programmes and services you must obtain their separate consent through an opt-in (which can be in the same original email, or a later edition of the newsletter) and explain what opting-in will mean. The Privacy Notice must be amended accordingly.
- Include a Privacy notice when you're collecting the information
- Always provide an unsubscribe notice with every communication explaining to individuals how they can unsubscribe
- Only use their personal information to send them that particular communication, unless you otherwise obtain their explicit consent
- Keep information lists safe and secure

MOD100018211

- Maintain accurate databases
- Once you no longer require the information i.e. the BBC programme ends, you should securely dispose of the information

3.2 Audience members

When we invite people to be audience members we may have to collect personal information about them. Sometimes we will also have to collect sensitive personal information, for example if they are appearing in the audience of a political or religious programme or if we need to get information about a person's studio access requirements because they have a disability.

You must:

- only collect the minimum information needed from each individual
- tell individuals what information the BBC is collecting by using a Privacy Notice at the time the information is collected
- be very careful about how the personal information is stored especially sensitive personal information
- only use the information for the specified purposes. If you are likely to wish to contact the audience for other purposes you will need to explain those purposes at the time of collection and obtain an opt-in consent
- only keep the information for the minimum time necessary
- follow the Contributor Guidelines if you want to use the details of an audience member to contact them about becoming a contributor in the future
- securely dispose of the personal information once you no longer require it

3.3 Contacting Message Board Users

Sometimes you might need to contact message board users about their posts, or wish to invite them to contribute to other BBC programmes. They may be contacted only with the email address they provided when signing up for Single Sign On.

The only people who are authorised to contact the message board users are the managers of the message board. If you are developing a programme and want to get in contact with a message board user, speak to the Message Board owner and request them to get in contact with the user. It is then up to the user to say whether they are happy for you to get in touch with them.

You may send them one email, and if after a week you do not get a reply from them you may try once more (just in case a person has accidentally deleted the email). If the person does not reply after the second email approach you should not contact them further. However, please be

aware that there are other circumstances where the BBC can legitimately contact users e.g. when a user is posting offensive content on a message board.

3.4 Competitions

The BBC has strict guidelines about how to conduct competitions. When you run a competition collecting personal information from entrants, you must also comply with the guidance in section 3.2 above. You should only keep the personal information for the minimum time necessary to properly run the competition. This means that you may need to keep information for a certain time afterwards in case there are any disputes about the conduct of the competition. However, that should be a reasonable limited time.

3.5 Consent

Consent means that the individual has "freely given" a "specific" and "informed" positive indication of their wishes to allow the BBC to use their personal information for a particular purpose or purposes.

For sending marketing or promotions, including newsletters and surveys, you should ensure that a user has checked an "opt-in" box (i.e. it is not enough to have a pre-populated check box which they must uncheck to refuse the data) agreeing to receive marketing or they have consented via an "I agree" or "subscribe" button.

3.6 Collecting Sensitive Information

"Sensitive Personal Information" is information that is deemed to be much more "personal" as to warrant extra protections. There are a number of specific categories of sensitive personal information defined by the Act - these are information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions.

It's important that you are aware of the special conditions to be fulfilled in relation to sensitive personal information. [See Rule 3] If you are collecting sensitive personal information, you need to obtain **explicit** consent from the individual (i.e. there must be no shadow of a doubt that the individual understands what information we are holding and for what purposes). [See Rule 4]

Remember:

- The BBC must have *explicit* consent from the individual agreeing to the way the BBC will be using this information
- Explicit consent must be in writing wherever possible. If not possible there has to be an unequivocal record (like a contemporaneous file note) of this explicit consent
- The BBC may be able to use sensitive personal information without explicit consent for limited purposes but you must contact the IPC Team in order to do so
- We must store sensitive personal information in accordance with higher Information Security criteria

MOD100018212

3.7 Collecting Sensitive Personal Information for Audience Access Requirements

Where information is collected about disability access requirements this qualifies as Sensitive Personal Information since information about a disability is health information.

When the BBC collects information about access requirements for individuals with disabilities you must:

- Only collect the information needed (e.g. you only need to know that the individual is in a wheelchair - not that they have a specific disease)
- Tell individuals *why* the BBC has to collect this information
- Store the information in a very secure place where only people with a genuine business need to know can access the information
- Do not disclose the information to any third party unless required to provide access to the individual. See Module 8 for the guidance on using third party data processors
- Delete the information when you have finished using it (i.e. after the programme has ended), unless there is a likelihood of continued access needs. In this case obtain explicit consent from the individual to keep the sensitive personal information and store securely. Refer to Module 9 - Security and Deletion of Personal Information for more on this.

3.7 Minimum Information Needed

You should only request the minimum information necessary. For instance:

- Is collecting a date of birth really necessary? Use age or age range instead
- Is collecting a full post code necessary? The first part is enough to check what region or area of the country the person lives in
- Is a full address necessary? For example, it may be necessary to deliver a prize or an information pack but not for other purposes.

3.8 Providing an unsubscribe notice

In every single communication (each email or text etc) you must provide the individual with a simple option to unsubscribe from receiving the marketing communication. This should be free to the individual (except for the cost of transmission). Unsubscribing from an email service should be via email and for text via return text (e.g. "Unsubscribe by texting "STOP" to 65555").

3.8 Receiving an unsubscribe request

When you receive an unsubscribe request from an individual you must:

- Act on the instruction as soon as possible (and in any event no later than 28 days)
- Remove all details of the individual on your main communications list EXCEPT for those details you need to retain as contact details on a "Suppression List"
- Maintain an accurate "suppression list" which is a list of people who have unsubscribed and who you should not contact with that specific marketing communication. You must check against this list to ensure that no materials are sent to individuals who have unsubscribed.

3.9 Limited use and deletion

You should only use the information for the particular purpose that you have collected it for [see Rule 6].

You must securely dispose of the information (including suppression lists) when the programme / website etc. is no longer operational.

Please also see Module 11 - Marketing for further background on rules around Marketing.

3.10 Individuals Rights

Don't forget that individuals whose personal information we hold still have rights to access the information or to ask for it to be corrected. We should try and ensure the information we hold about individuals is as up to date and accurate as possible. See Module 14 - Subject Access Requests and Module 16 - Complaints for more information.

3.11 Privacy notices and guidance

When the BBC collects personal information from individuals you must always be clear about *what* information you are collecting and *why*.

This should be set out in a Privacy Notice which is a short statement that explains:

- *what* information we are collecting;
- *why* information is being collected;
- *every purpose* for which the information is collected;
- *who will be using the information* i.e. the BBC and mention any other third parties who will have access to or otherwise use the information. You need not list all third party service providers but you should provide details of third parties who will be accessing the personal information who are not service providers to the BBC; and
- any other information about *how the information will be used* which would be necessary to ensure that the use by the BBC of this information is fair.

This information can be interspersed within the text of the website if you are collecting information online but it must be easy for the user to find. However, it is not acceptable to require the user to click away from the information collection webpage to a separate webpage

which contains the Privacy Notice like the T&Cs.

3.12 Privacy Notice Examples

When information is gathered and used by the BBC only and not passed on to any other parties.

A. Emails:

The information you provide will be collected and compiled by BBC researchers for the next series of [INSERT PROG NAME]. They will only use your personal details for the purposes of contacting you about the programme. Your personal information will be treated in accordance with the Data Protection Act 1998. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

B. Photos:

The BBC may wish to publish your photograph and message on the BBC website or during the programme. You need to ensure that your submission adheres to the BBC's Terms of Use. The BBC's [INSERT PROG NAME] production team will retain your photograph and contact details and will only use your contact details to contact you with regard to your submission and its use by the BBC. Your details will not be passed to anyone else. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information. We cannot guarantee that your photograph will be shown on the programme or the website.

If you submit a photo that shows anyone other than yourself, you must obtain their permission first and if the person is a child you will need to obtain their parent's written consent.

C. If photo is being used only on the website:

The BBC may wish to publish your photograph and message on the BBC website. You need to ensure that your submission adheres to the BBC's Terms of Use. The BBC's [INSERT WEBSITE NAME] online team will retain your photograph and contact details and will only use your contacts details to contact you with regard to your submission and its use by the BBC. Your details will not be passed to anyone else. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

If you submit a photo that shows anyone other than yourself, you must obtain their permission first and if the person is a child you will need to obtain their parent's written consent.

D. Videos:

If video is being used only on the website:

The BBC may wish to publish your video and message on the BBC website. You need to ensure that your submission adheres to the BBC's Terms of Use. The BBC's [INSERT WEBSITE NAME] online team will retain your video and contact details and will only use your contact details to contact you with regard to your submission and its use by the BBC. Your details will not be passed to anyone else. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

If you submit a video that shows anyone other than yourself, you must obtain their permission first and if the person is a child you will need to obtain their parent's written consent.

We might like to contact you about your post.

E. Phone number

Your information will be collected by the BBC's [INSERT PROG NAME] team. They will only use your personal details for the purposes of contacting you about the programme. Your personal information will be treated in accordance with the Data Protection Act 1998. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information. If you have any other queries then please go to the Contact Us page.

F. Contact Us pages

The details you supply will be treated in strictest confidence and will only be used by BBC for the purposes of contacting you about the query/comment etc that you have made. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

G. Newsletters

Your email address will be held by the BBC and kept confidential, and will only be used in relation to this newsletter. You will be given the option to unsubscribe from this newsletter each time you receive it. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

H. Competitions (see these Guidelines also)

The BBC will only use your personal details for the purposes of administering this competition, and will not publish them or provide them to anyone not connected with this competition without your permission. If the BBC is required to pass your details to any third party for the purposes of administering this competition, the BBC will require that they only use your details strictly for these purposes. If you would like to know more about the BBC's Privacy & Cookies Policy, please see Privacy Policy.

Where information is collected or passed on to Indies and Externals

Note that if the website is being hosted externally by the Indie then the BBC's Privacy & Cookies Policy might not apply. If the Indie in question has a Privacy Policy, you should refer to it in the Privacy Notice. If the information will be sent to the BBC first and then passed on to the Indie, then the BBC's Privacy & Cookies Policy will apply.

Remember that the BBC must have a written data processing agreement in place with any Indie who collects personal information on the BBC's behalf. You must be satisfied that the level of security they offer for the personal information is suitable. Speak to your DP Representative or IPC for advice. [See Rule 13 and Rule 14]

A. Email:

Example 1

Please note your information will be sent to [INSERT INDIE'S REGISTERED COMPANY NAME], producers of the series [INSERT PROG NAME]. [INSERT INDIE] will only retain and use the information you provide for the purposes of the [INSERT PROG NAME] programme, and will share the information only with the BBC for those purposes, and not with any third parties. The BBC is the Data Controller for the purposes of collecting this data. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

Example 2

Your application will be sent to [INSERT INDIE], independent producers commissioned by the BBC to make [INSERT PROG NAME]. [INSERT INDIE] will only retain and use the information you provide for the purposes of the programme, and will share the information only with the BBC for those purposes, and not with any third parties. The [INSERT PROG NAME] production team at [INSERT INDIE] and the BBC will only use your contacts details to contact you with regard to your application. Your details will not be passed to anyone else. If you have any other queries then please go to the Contact Us page. The BBC is the Data Controller for the purposes of collecting this data. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

B. Photos:

Your photographs and contact details ("information") will be sent to [INSERT INDIE], producers of [INSERT PROG NAME]. [INDIE] will only retain and use the information you provide for the purposes of the programme, and will share the information only with the BBC for those purposes, and not with any third-parties. The BBC may also wish to publish your photograph and/or message on the BBC website [INSERT URL]. You need to ensure that your submission adheres to the BBC's Terms of Use (www.bbc.co.uk/terms). The [INSERT PROG NAME] production team at [INSERT INDIE] and the BBC will only use your contacts details to contact you with regard to your submission and its use. Your details will not be passed to anyone else. We cannot guarantee that your photograph will be shown on the programme or the website. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

If you submit a video that shows anyone other than yourself, you must obtain their permission first and if the person is a child you will need to obtain their parent's written consent.

C. Videos:

Your videos and contact details ("information") will be sent to [INSERT INDIE], producers of [INSERT PROG NAME]. [INDIE] will only retain and use the information you provide for the purposes of the programme, and will share the information only with the BBC for those purposes, and not with any third-parties. The BBC may also wish to publish your video and/or message on the BBC website [INSERT URL]. You need to ensure that your submission adheres to the BBC's Terms of Use (www.bbc.co.uk/terms). The [INSERT PROG NAME] production team at [INSERT INDIE] and the BBC will only use your contacts details to contact you with regard to your submission and its use. Your details will not be passed to anyone else. We cannot guarantee that your video will be shown on the programme or the website. Please visit the BBC's Privacy & Cookies Policy (www.bbc.co.uk/privacy) for more information.

If you submit a video that shows anyone other than yourself, you must obtain their permission first and if the person is a child you will need to obtain their parent's written consent.

D. Phone number:

Your information will be sent to [INSERT INDIE], producers of [INSERT PROG NAME]. [INSERT INDIE] will only retain and use the information you provide for the purposes of the programme, and will share the information only with the BBC for those purposes, and not with any third-parties. The [INSERT PROG NAME] production team at [INSERT INDIE] will only use your phone number to contact you with regard to your submitted question. Your details will not be passed to anyone else.

E. BBC to external party, then transferred to a third party:

NB always check with the Indie how they will collect and use the personal information and whether any third parties are involved. If they will be sharing information with another third party then use the wording below. We must always make it clear who will be holding individuals' personal information. Your agreement about collection and processing of information must be in writing.

Your email will be sent to [INSERT INDIE], independent producers commissioned by the BBC to make [INSERT PROG NAME]. [INSERT INDIE] will only retain and use the information you provide for the purposes of the programme, and will share the information with only one third party - [INSERT THIRD PARTY NAME] - which [INSERT INFO ABOUT THIRD PARTY]. [INSERT THIRD PARTY NAME] will only use your contacts details to contact you with regard to your email. Your details will not be passed to anyone else.

F. Linking to external website

This is not a Privacy Notice as such, but you need to add a line of text after the link to external website.

To apply online, go to [INSERT EXTERNAL WEBSITE URL]. The BBC is not responsible for the content on external websites and BBC recommends that you check their privacy policy about how they plan to use your personal information. Some sites may send or host your personal information outside the European Economic Area.

Module 4 - Contributors and User Generated Content

SUMMARY

If you want to use details about contributors including their contributions or UGC you must:

- obtain their consent to send them marketing information
- allow them the ability to opt out of receiving marketing information
- obtain their consent to invite them to contribute to other programmes
- only collect the minimum information necessary
- provide a Privacy Notice

Everyday across the BBC we collect, use and store information about our contributors - from experts in various fields, to schoolchildren, to people off the street. These contributions often contain information about other people as well as about the contributors themselves.

Using contributors on your programmes and obtaining their consent is governed by the Editorial Guidelines.

We also collect information provided by users to websites as User Generated Content.

4.1 Contributor personal details

When you collect personal information about contributors you must:

- only collect the minimum necessary, although this may be quite detailed for legal and editorial reasons; for example, only collect age if it's strictly necessary for your story, e.g. the pension crisis.
- tell individuals what information the BBC is collecting from them. As far as possible, you should include a Privacy Notice when collecting personal information. However, it is recognised that in daily news and equivalent environments it may not be possible to collect more than initial contact details. If you wish to keep the contact details for future use, seek their consent and wherever possible you should obtain this consent in writing via the Contributor Data Collection Form.
- only use the information for the specified purpose(s) for which they have been collected unless you have the individual's consent to use the information for another purpose (e.g. to invite them to take part in another show or a future show)
- keep all contributors' personal information safe and in line with BBC Information Security guidelines (especially where you are collecting sensitive personal information or children's information).
- only keep the information for the minimum time necessary to fulfil our purpose(s) and once you no longer require the information you should securely dispose of it

Can I pass contributor personal details to another BBC Programme or an Indie?

If the contributor has consented to this when they completed the contributor database form then you may pass this information to another BBC Programme. Otherwise you should not share their information within the BBC. You should not make the personal details available outside the BBC.

If you send details to an Indie, it is likely that they will be acting as a *data processor*. This means that you must ensure that there is a written contract in place that sets out that the Indie will only use the details for the BBC programme that they are producing, and will only process the information in accordance with the BBC's instructions. See Module 7 - Working with Indies for more details.

However, there are circumstances where the Indie will be acting as a *data controller* and will use the personal information for its own purposes. The Indie is then required to ensure that it uses the personal information in accordance with the DPA.

If you are unsure about passing the details to an Indie, you should contact the individual and seek their consent to pass their details on (you should only contact them once. If they don't respond assume their answer is "no").

Example: BBC History are making a programme on a military hospital which is due to close down. They found an account on the People's War website from someone who had worked at the hospital, and asked for the individual's contact details. As the individual had been told that her information would be used only in connection with People's War, we asked the People's War team to contact her and ask if she would be happy for them to pass on her details to the BBC History team. This ensures that the individual is able to control how her personal information is used.

The full Guidelines for Collecting and Storing Contributor data are available on the IPC Gateway site.

4.2 User Generated Content Contributors

If you wish to contact the contributors of user generated content then you must make them aware of this when they upload their content. (e.g. "We may use your personal details to contact you in relation to your submission. Please see our Privacy Policy for more information.").

You should only contact people in relation to the content they have uploaded unless they specifically consent to you contacting them for other purposes - see Module 11 - Marketing.

You should be aware that there are other legal issues around User Generated Content such as where the content provided by the user infringes the copyright of a third party or the content provided is defamatory of another person. Please contact Programme Legal Advice for further information.

4.3 Text messages

MOD100018216

When the BBC receives text messages from users it receives personal information about individuals in the form of the sender's phone number as well as any personal information included in the content of the message.

Module 5 - Children's and Young People's Personal Data

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 Privacy 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 IPC 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

BBC Children's have set their own departmental guidelines for the appropriate lengths of time that personal details should be kept, depending on the purpose it was collected for. Departments other than BBC Children's should adhere to the same retention periods.

If you are not sure of how long you should keep children's data please contact IPC or your Data Protection representative.

Module 6 - Launching a Website

SUMMARY

If you want to launch a website either associated with the BBC or externally you must:

- Consider whether you are collecting personal information
- Ensure that you have obtained the necessary approval if a third party is hosting the website
- If personal information is being transferred outside the EEA obtain approval from the IPC Team
- Use Privacy Notices and Privacy Policies when collecting personal information

6.1 Are you collecting personal information?

If you are collecting personal information you must refer to Module 3 - Contacting the Audience. If you permit users to provide User Generated Content you must refer to Module 4 - Contributors and User Generated Content. If no personal information is being collected this module does not apply.

6.2 Is the website being hosted by a third party?

If so you must comply with the Third Party Hosting Guidelines, and ensure that the third party completes the Information Security hosting questionnaire both of which can be found at http://www.bbc.co.uk/guidelines/newmedia/infrastructure/third_party.shtml

You should consider:

1. Are you passing the personal details onto another party to use on the BBC's instructions or is another party collecting the personal details on the BBC's behalf? If yes, see the Data Processors module 8. If not, and the third party is using the personal information for their own purposes, please see Module 8 - Working with Data Processors. If the third party is not an Independent Production Company, please contact Information Policy and Compliance to discuss.

2. Are you using any cookies on your site? You must notify new cookies in accordance with the Cookies Standard so that it can appear on the Cookies List (see BBC Privacy and Cookies Policy).

6.3 Transferring personal information outside the EEA

It is important that the BBC does not transfer personal information outside the EEA (the European Economic Area - which is made up of the countries listed below) unless there are

adequate controls in place to secure the safety of the information. Transfers within the EEA are considered to be safe. [See Rule 13 and Rule 14] The ONLY way in which a transfer of personal information is acceptable is as follows:

- With the explicit consent of each individual whose information is being transferred;
- If the company to whom the information is being transferred is in the US and the company is registered with the "Safe Harbor" regime. For more information on Safe Harbor see: www.export.gov/safeharbor
- If there is a written contract in place that includes acceptable "model clauses"; or
- With the express consent of the BBC Data Protection Officer.

You should be aware that the use of a server outside the EEA to *host* the website is considered transferring personal information. Please check contracts with third parties in the EEA to ensure that they do not sub-contract services to companies outside the EEA. If there is nothing in the contract, ask the third party to confirm whether or not they use sub-contractors based outside the EEA and ensure that they provide a clear response to this query as they may try to side-step the issue. If a third party does use overseas subcontractors you must ensure that you obtain the approval of the IPC Team before any contract that would include such a transfer outside the EEA is signed.

The UK regulator, the Information Commissioner, considers that transfers to the following countries provide adequate safeguards:

- Argentina
- Canada
- Guernsey
- Isle of Man
- Switzerland

Consequently, a transfer of personal information to these countries and territories can be treated in the same way as a transfer within the EEA. The EEA comprises the 27 countries within Europe (UK, France, Germany, Spain, Portugal, Austria, Italy, Greece, Hungary, Czech Republic, Slovakia, Slovenia, Latvia, Estonia, Lithuania, Romania, Bulgaria, Sweden, Denmark, Finland, Malta, Poland, Ireland, Belgium, Cyprus, Luxembourg and the Netherlands) and Iceland, Norway and Liechtenstein.

However for other countries, a data transfer agreement based on the EC Model Clauses will need to be agreed with the supplier and specific additional security measures will need to be put in place.

Further information about this can be found at:

www.ico.gov.uk/upload/documents/library/data_protection/practical_application/generic_guidance_international_transfers_v2.pdf

6.4 Privacy notice

Users should be given sufficient information to help them understand *why* personal information will be collected from them if they use the website and *for what purpose*. See Module 3.11 and 3.12 - Contacting the Audience for guidance on Privacy notices and Privacy Policies. You should ensure that the website functionality is designed so that you only collect relevant and necessary information. Where users are allowed to provide User Generated Content, you should refer to

MOD100018219

For Distribution to CPs

6.5 Individuals Rights

Don't forget that individuals whose personal information we hold still have rights to access the information or to ask for it to be corrected. We should try and ensure the information we hold about individuals is as up to date and accurate as possible. See Module 15 - Data Security Breaches and Module 16 - Complaints for more information.

6.6 Deletion

Where the website is to be closed, you must delete the information that you have received from contributors. For further information see Module 4 - Contributors and User Generated Content.

Module 7 - Data Protection Guidelines for Independent Production Companies

SUMMARY

When using an independent production company you must:

- Ensure Indies are aware of their responsibilities under this Handbook whether they are a data controller or data processor
- Only collect necessary and relevant information from individuals
- Use Privacy Notices
- Ensure that Indies comply with BBC Information Security requirements
- Consider whether personal information will be sent outside the EEA
- Comply with the rules around using information for a different programme
- Ensure that the rules around using sensitive personal information and children's information are followed if relevant

7.1 Data Protection Guidelines for Indies

These guidelines are aimed at Indies producing programmes for the BBC.

In the course of producing the Programme you may need to collect and process personal data in your own right (as a Data Controller) and/or on behalf of BBC (as a Data Processor).

Here are some examples where you might be dealing with personal data:

- If you are hosting a website where contributors register with your site and they contribute to message boards or similar offerings
- If you are promoting BBC content or services directly to the public (eg via an email newsletter)
- If you are producing a game show and are collecting contact information from potential contestants and contestants
- If you are running an interactive phone-in or competition and you are keeping a record of the phone numbers of people who have called in
- If you are inviting contributors to send user generated content, such as photographs or video clips

Where you do it's important that you comply with the PPA, the Data Protection Act ("DPA"), all relevant BBC Guidelines including Editorial Guidelines, and these Guidelines. Please note that

MOD100018220

there are some circumstances where the BBC will require you to comply with a higher standard of protection of personal data than the DPA.

When you collect personal data in order to produce the Programme you will be considered either a "Data Processor" (where BBC is the "Data Controller"), the sole Data Controller or joint Data Controller (with BBC and possibly others) under the Data Protection Act.

7.2 What is a Data Controller?

The Data Controller is a person (individual or company) who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Where YOU decide what personal information is going to be kept; and the use to which the information will be put YOU will be the data controller. Where the BBC and You decide the manner in which the data will be processed then You and the BBC will be joint Data Controllers.

Individuals about whom you collect data must be clear that You and not the BBC is the data controller. Further - you will be required to comply with the Data Protection Act 1998.

7.3 What is a Data Processor?

The Data Processor is any organisation which processes data on behalf of the Data Controller.

You are the Data Processor if you do not exercise responsibility for or control over the personal data - ie you act on direct instructions from the BBC.

7.4 Are we (the Producer and the BBC) Joint Data Controllers?

There are times where both will be the data controllers and the BBC and you jointly decide what personal information is going to be kept; and the use to which the information will be put. In such cases there may be additional contractual provisions that set out the expectations and limits within which each party may process the personal information.

Your commissioning specification should indicate who is the Data Controller and who is the Data Processor

7.5 What is personal information?

Personal information is any information that relates to a living individual who can be identified:

- from that information or
- from that and other information in your or the BBC's possession or likely to come into your or the BBC's possession.

7.6 Personal information can include:

- an email address or telephone number, collected for example when people enter competitions, sign up for a newsletter or become part of a programme's database of contributors.
- information about people's personal experiences and opinions we collect for use online, on TV or on radio.

7.7 What is sensitive personal information?

Sensitive personal data includes information about: ethnic or racial origin; political opinion; religious or other similar beliefs, e.g. agnosticism, atheism; trade union membership; physical or mental health details; sexual life e.g. sexual orientation; or alleged or proven criminal or civil offences.

Medical information includes disability. Therefore if information is collected about disability access requirements this qualifies as Sensitive Personal Data

7.8 What information can I collect?

You should only request the minimum information necessary. Think about :

- whether collecting a date of birth is really necessary. Use age or age range instead
- whether a full post code is necessary. The first part is enough to check what region or area of the country the person lives in
- whether a full address is necessary. For example, it may be necessary to deliver a prize or an information pack but not for other purposes.

7.9 What must I tell people when I'm collecting information about them?

You must be very clear with individuals about *what data* you are collecting and *why*. You should always include a "Use of Data" notice - you must always explain every purpose for which the information will be collected before it is collected. You must also explain *who* will be holding it ie when you are the Data Processor that it will be your company on behalf of the BBC and mention any other third parties who will have access to or otherwise use the data. If third parties are to have access to or otherwise use the data their use must always be subject to these guidelines & when you are the Data Processor the BBC's prior knowledge and consent is essential.

Where you are the Data Controller you must ensure that you comply with all the conditions of the Data Protection Act. Please also note your contractual conditions not to bring the BBC into disrepute in any way.

7.10 How should I store the data?

MOD100018221

You must ensure it is stored securely in accordance with the BBC's Information Security guidelines. These are available online at http://www.bbc.co.uk/guidelines/dq/contents/information_security.shtml

7.11 What about sending data overseas?

You must not send personal data outside the European Economic Area without the express written permission of the Information Policy and Compliance department of the BBC. This includes sharing data with any parent or affiliated company and may include functions such as websites that are hosted in the USA.

7.12 For how long can I store the data?

Personal information should only be kept for the minimum length of time necessary and appropriate to the uses for which it has been agreed. For example, once a quiz series has ended you won't need to keep personal data in relation to people who applied to be contestants but weren't chosen. If you need data for auditing purposes, etc, it is acceptable to keep it, but the length of time must be justified by a specific business need.

7.13 Do I need to do anything else with the data?

You must ensure where it is necessary to keep the data for more than a short time that you keep the information up to date and accurate. For example, you can provide an email address for individuals to notify of any changes to their details.

7.14 What do I do with the personal data once it's no longer of any use?

Once the purpose for which the information has been used has come to an end, it must be disposed of securely as follows:

Manual Data

- Information should only be deleted/destroyed by those people with the required authority (e.g. for some children's personal information, this information can only be deleted by someone who has passed a criminal records bureau (CRB) check).
- It is important that manual files including personal information are properly shredded or disposed of as confidential waste. Where personal information can be obtained from the document, it should be shredded or otherwise confidentially disposed of. If you have any questions about how to dispose of manual waste please contact dpa.officer@bbc.co.uk or ism@bbc.co.uk.

Electronic Data

- You must ensure that our processes meet the minimum standard for the "destruction of data stored in electronic form" which is that it should be **reformatted or overwritten** such that all personal information is permanently, completely and irretrievably

destroyed. This includes all copies of the data from all systems although there may be circumstances where it is appropriate to retain a copy on back-up systems;

- You must perform adequate checks after the destruction of electronic data to ensure that all applicable data has been properly deleted;
- The process of deleting electronic data, and the subsequent audits that this deletion requires, must only be performed by those people who are authorised to access the personal information included in the electronic data (including, where applicable, sensitive personal information) within the third party organisation (e.g. only people who have passed adequate checks to deal with children's information must deal with its deletion)

7.15 What if I am engaging a third party to handle personal data for the Programme?

If you are using a third party to process personal information on your behalf you must ensure that they abide strictly by these guidelines and that your contract with them reflects the contractual responsibilities you have with the BBC about the handling of personal data. Third party processors should comply with the specific responsibilities set out in these guidelines relating to data processors.

7.16 Can I use the personal data for our other projects or for marketing?

In limited circumstances it may be reasonable to use a database for other BBC projects but this will require the following:

- Specific and detailed consent from the individuals (refer to Contributors Guidelines)

  (e.g. *you agree to let us use the details for your participation in this year's Crufts programme. We may wish to approach you using these details inviting you to participate in any other programme about Dog Shows in the next [X] years. If you agree to be contacted for this purpose please check here [ ]*
- A mechanism for keeping the personal information up to date and accurate
- At the end of the specified period the personal information must be deleted

7.17 For Data Processors:

You must only use the personal data for the purposes of the Programme and not for any other use. This means that you must not sell, distribute or provide in any other form to any third party this data, except where this is necessary to produce the Programme and you have informed the individual that you will process the data in this manner.

You must not use the data for any other projects with which you're involved. In limited circumstances it may be OK to use a database for other BBC projects but this will require the following:

- Specific and detailed consent from the individuals

MOD100018222

(eg you agree to let us use the details for your participation in this year's Crufts programme. We may wish to approach you using these details inviting you to participate in any other programme about Dog Shows in the next 3 years. If you want to be contacted for this purpose please check here [ ])

- A mechanism for keeping the data up to date and accurate
- At the end of the specified period the data must be deleted (see above)

7.18 For Data Controllers:

When you are the sole Data Controller You are responsible for making decisions about how you use the data you collect.

7.19 What are the additional requirements if I'm processing sensitive personal data?

In order to process sensitive personal data you will normally need to gain the "explicit consent" of the individuals. This means that your "use of data" notice must be detailed and specific and the individual is seen to understand exactly why and for what the sensitive information is being collected and processed. General consents will not be appropriate in such instances. Examples of when sensitive personal data is collected include current affairs applications where we may ask for details regarding disabilities, ethnic background, political affiliations or criminal convictions. Sensitive personal data must always be gathered on a very limited basis and access to it very strictly controlled; consider whether everyone on your team needs to see this particular data to carry out their job.

There may be circumstances where if you are collecting personal information specifically for journalistic purposes you may not need the explicit consent of individuals to comply with the Act. In such cases you must adhere strictly to the editorial guidelines and gain the relevant approvals to conduct activities such as secret filming.

7.20 What about children's data?

As with sensitive personal data, we have to be very cautious about the collection of children's personal data and children's ability to give consent for their data to be passed to you and used on the BBC's behalf. If your commission with the BBC will involve the collection and use of children's personal data, the processes for this must be discussed and agreed with the BBC before any data collection starts.

The BBC will often require parental consent when collecting children's data, the nature of this consent will depend on the exact nature of the programme, project or website. You should make sure you consult on a case by case basis with the BBC to ensure the appropriate steps are taken in any situation where children's data is to be collected. You should contact your BAM in the first instance, who will ensure that guidance from the BBC's Information Policy and Compliance department is provided for each project either by putting you in contact with the IPC team direct or by liaising with them on your behalf.

7.21 Does my company need to notify the Information Commissioner that we will be acting as a Data Processor or Data Controller?

It is extremely likely that your company needs to register with the Information Commissioner just to carry out its own business in any event. If you are acting as a Data Controller it is most likely that you will have to register with the Information Commissioner.

Please refer to the ICO's website for more information about notification:
http://www.ico.gov.uk/what_we_cover/data_protection/notification.aspx

7.22 Where can I find more information about Data Protection?

Please remember that you must always rely on your own legal advice and not of that provided by the BBC. However, there are lots of resources on www.ico.gov.uk that will tell you about what's happening in the world of Data Protection.

The BBC's Information Policy and Compliance department can be contacted at:
dpa.officer@bbc.co.uk

The BBC's Information Security Team can be contacted at: ism@bbc.co.uk

MOD100018223

Module 8 - Working with Data Processors including Outsource Service Providers

SUMMARY

When using a data processor you must

- Be aware that the BBC remains responsible under the law for the data processor's actions
- Put in place a written contract between the BBC and the data processor
- Ensure that the data processor will put appropriate security measures in place to protect the personal information

8.1 The responsibility of the BBC

When we work with any data processors, whether they are outsourced service providers, Indies, web processing sub-contractors or others, it is important to remember that the BBC remains responsible for data protection compliance and for compliance with this Handbook. This means that we must be very careful and thorough when providing guidance to data processors.

8.2 The need for a written contract

The BBC controls what a data processor can do with the personal information they collect on our behalf through a written contract. You must not allow any third party to process BBC (including audience) personal information without a written contract being in place and signed by the BBC and the data processor who agrees only to use personal information as instructed by the BBC. Please contact the IPC Team for details of what needs to be included in the contract.

8.3 Required security measures

The data processor must also have appropriate security and technical measures in place to protect personal information. You must review their IT and other security measures to ensure these are satisfactory. As well as their technical security, we need to ensure that they employ reliable staff who are properly trained. You should contact the IPC Team if you need help deciding whether a proposed data processor meets the BBC standards.

In carrying out this exercise, you should identify:

- What personal information will the data processor be using?
- What is the actual processing? For instance, is the data processor only storing the information or will they be collecting, sorting or otherwise changing the information?
- Whether the data processor has a data protection and/or privacy policy (if they don't, they should have)
- Who within the data processor's company will be accessing the personal information?
- How will the data processor ensure the reliability of their staff?
- What training is in place for staff? The BBC should reserve the right to approve training.
- What technical security measures will be used to protect the personal information?
- What manual security measures will be used to protect the personal information? (e.g. how should hard copy personal information be posted?)
- A Personal Information map that covers all possible movements of personal information within the relationship between the BBC and the data processor (Contact IPC if you require assistance with this).

The technical and organisational security measures must comply with the BBC's security policies as set out by BBC Information Security from time to time.

Where the data processor or outsource service provider is located *outside the EEA* you must contact the IPC Team for specific guidance and sign-off.

MOD100018224

Module 9 - Security and deletion of personal information

SUMMARY

It is an essential requirement that the BBC and any data processors keep personal information secure. In ensuring the security of personal information, you must

- Ensure that access to information is only given to those who have a business need
- Ensure that personal information is only kept for as long as is necessary and is deleted once it is no longer needed

9.1 How do I keep Personal Information secure?

Only people who have a genuine business need to know should be able to access personal information. All files containing personal information must be adequately protected by passwords and encryption in accordance with the BBC's Information Security Policies.

Check out the Top Tips for Information Security. For advice about laptop encryption speak to the Technology Service Desk on 02 26333.

9.2 Deletion of Information

It is important that personal information is only kept for the minimum time necessary to fulfil the purposes for which it was collected. [See Rule 10] Additionally when we delete systems or files with personal information or sensitive personal information, we must ensure the following:

Manual Data

- Information should only be deleted/destroyed by those people with the required authority (e.g. for some children's personal information, this information can only be deleted by someone who has passed a criminal records bureau (CRB) check).
- It is important that manual files including personal information are properly shredded or disposed of as confidential waste. Where personal information can be obtained from the document, it should be shredded or otherwise confidentially disposed of. If you have any questions about how to dispose of manual waste please contact the IPC Team or Information Security.

Electronic Data

- We must ensure that our processes meet the minimum standard for the "destruction of data stored in electronic form" which is that it should be **reformatted or overwritten** such that all personal information is permanently, completely and irretrievably destroyed. This includes all copies of the data from all systems although there may be circumstances where it is appropriate to retain a copy on back-up systems.
- We must perform adequate checks after the destruction of electronic data to ensure that all applicable data has been properly deleted.

- The process of deleting electronic data, and the subsequent audits that this deletion requires, must only be performed by those people who are authorised to access the personal information included in the electronic data (including, where applicable, sensitive personal information) within the third party organisation (e.g. only people who have passed adequate checks to deal with children's information must deal with its deletion).

If you have any questions about this please contact the Information Policy and Compliance team at DP Advice or ISM@bbc.co.uk

9.3 Deletion of Information by Third Party Data Processors

When third parties are processing information that includes personal information we must ensure the following when deleting systems or files:

Third parties

- Third parties must meet the minimum standard for the "destruction of data stored in electronic form" which is that it should be **reformatted or overwritten** such that all electronic data is **permanently, completely and irretrievably destroyed.** This includes all copies of the data from all systems although there may be circumstances where it is appropriate to retain a copy on back-up systems.
- Third parties must perform adequate audits after the deletion of the electronic data to validate the fact that all applicable data has been destroyed. A record must be kept of these audits which the BBC can inspect upon reasonable notice.
- The process of deleting electronic data, and the subsequent audits that this deletion requires, must only be performed by those people who are authorised to access the personal information included in this electronic data (including, where applicable, sensitive personal information) within the third party organisation (e.g. only people who have passed adequate checks (CRB) to deal with children's information must deal with its deletion).
- Third parties must provide the BBC with a written undertaking that these measures have been followed before any hardware that has held or is otherwise associated with the personal information is disposed of or utilised for any other purpose.
- Although the BBC reserves the right to audit any systems on which electronic data was held for the purposes of satisfying itself that the data has been destroyed, it shall be under no requirement to do so.

Module 10 - BBC People and Personal Information

SUMMARY

Managing personal information is everyone's responsibility. In using personal information about BBC staff, you must

- Understand on what basis the BBC can use employee personal information
- Ensure that individuals are vetted to the appropriate level e.g. including CRB checks
- Ensure that employee information is only accessible to the relevant people including health information
- Put in place a procedure for taking employee personal information outside the BBC

The BBC as an employer, and all people who work at the BBC have responsibilities under the DPA. No one should disclose personal information in breach of the BBC's procedures or use any personal information for their own purposes.

Please note that a serious infringement of data protection rules when handling employee personal information is a disciplinary matter and may be a criminal offence.

10.1 Introduction

This module sets out what information the BBC holds about you if you are a BBC employee or member of staff as a freelancer or contractor and how it is used, and also provides guidance on how you must process employee information if you are a manager or otherwise required to deal with employee information as part of your role at the BBC.

10.2 Why does the BBC collect personal information about employees?

The BBC collects and uses personal information about employees for a number of purposes and at all stages of the employment lifecycle.

These purposes are:

- Recruitment - including verification and vetting (CRB checks)
- Employment administration - appointments and removals, payroll, emergency contact details, occupational health details, training & development, appraisals, disciplinary matters and grievances
- Pensions
- Organisational Risk Management

10.3 Recruitment

Job applications are made on the BBC's online recruitment system or via third party recruitment agencies. Details registered on the BBC's online system by applicants remain on file for six months and are then deleted unless the applicant opts to extend this period. Unsuccessful applicants' forms are held for three years.

Successful applicants' forms are transferred to their personnel file and retained in line with the Corporate Retention Schedule.

Verification and Vetting

The BBC undertakes the following verification and vetting activities:

- References are taken for all staff and become part of their personnel file.
- The BBC will ask to see your passport or other immigration documents to ensure you have a right to work in the UK.
- Additionally, staff recruited to work with children or vulnerable adults may be subject to a CRB check.

10.4 Criminal Record Bureau Checks

Details and forms for CRB checks can be found at the Working with Children intranet site

As an integral part of its Child Protection Policy, the BBC is registered with the Criminal Records Bureau (CRB) as a Registered Body who can countersign applications for CRB checks and receive the Disclosure results. The CRB is an executive agency of the Home Office and provides access to criminal records and other related information (see www.crb.gov.uk). The CRB's role is to assist employers to make considered recruitment decisions where staff are working with children, young people or other vulnerable groups.

Under the provisions of the BBC's Child Protection Policy, where a new recruit or current member of staff will be working closely with children, a CRB disclosure form must be completed. The BBC is required to comply with the CRB Code of Practice.

Disclosure application forms can only be signed off on behalf of the BBC and sent to the CRB by specific people authorised by the CRB for this purpose. These people are known as 'counter signatories' and a list of such people is available at the Working with Children intranet site

How is the Disclosure used?

The CRB produce two copies of the Disclosure in response to the application form. One is sent to the applicant at their home address. The other is sent to the counter signatory within the BBC who reviews the Disclosure.

The counter signatory keeps a protected electronic record of the date of issue of a Disclosure, the name of the individual, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the recruitment decision taken.

The CRB Disclosure forms themselves are kept in a secure place for 6 months and then shredded unless there is an exceptional reason to keep the Disclosure for longer than 6 months.

Who can access the Disclosure?

The Disclosures are reviewed by the counter signatories in order to make a recruitment decision. Disclosure information should only be passed to those parties who are authorised by law to receive it in the course of their duties (this is a requirement under s. 124 Police Act 1997). Please contact the BBC Lead Countersignatory (Head of Employment Policy) for further information. You should be aware that it is a criminal offence to pass Disclosure information to anyone who is not entitled to receive it.

How should Disclosure information be stored:

It is a requirement of the CRB's Code of Practice that all Registered Bodies such as the BBC must have a written policy on the correct handling and safekeeping of Disclosure information see how the BBC stores and disposes in the BBC Policy Statement: Secure Storage, Handling, Use, Retention & Disposal of Disclosures and Disclosure information.

10.5 Employment Administration

The personal information that employees supply to the BBC is used to administer the employment relationship. Only details that are needed to administer this relationship must be collected. The BBC and the employee must ensure that these details are kept accurate and up to date.

The information should only be disclosed to people who have a genuine business need or legal right to see it. This may include your line manager and our external service partners (e.g. for payroll purposes).

It may also be shared with or passed to other organisations within the BBC family should you transfer between the Corporation and/or its subsidiary companies (e.g. BBC Resources, BBC Worldwide) in order to ensure the continuity of your employment record.

In most cases the personal file is now held in electronic format. You have a right to see your personal file and the other information that we hold on you.

You can also see (and change) key personal information that we hold on you via myDetails, which can be accessed via Gateway.

10.6 Occupational Health

This organisational risk management function is largely outsourced to HR Direct which is managed by Capita (as a data processor). Medical information is held and accessed only by clinical staff. The purpose of holding the information is to provide an occupational health service to the BBC.

Access to occupational health records is restricted to the BBC's Chief Medical Officer and the Principle Risk Manager, Occupational Health. If you have any questions about your own occupational health record, or access to other records please contact Occupational Health.

Capita HR Direct holds medical records for current and past BBC employees as the BBC's data processor. Access to these records is restricted to clinical or authorised medical staff.

Records are stored on the Corporate Health and Safety management system (Chrysalis) - a secure database with restricted access.

10.7 Organisational Risk Management ("ORM")

The ORM team manage the myRisks system for recording workplace accidents. The system is held on a secure server

This system holds a feed of basic information from SAP which includes personal identifiers and organisational assignment (e.g. name of individual and name of line manager).

To this is appended accident reports including the following information: name, address, sex and age of injured or otherwise involved parties - staff and members of the public - and the nature of any injuries incurred.

Access to this information is restricted to the line management chain for managing the resolution of the incident and the ORM Team to provide assistance and to complete statutory reporting.

10.8 Capita HR Direct

Capita HR Direct is the BBC's outsource service partner and data processor for certain human resources functions. On behalf of the BBC, they collect and maintain the bulk of the information used for HR purposes. They are contractually obliged to maintain and use it only as per BBC instructions. Access to the information by individual members of HR Direct staff is agreed formally with the BBC.

Before releasing information to members of staff or line managers, they must confirm their identity using approved security questions.

Information is only released to managers according to processes agreed with the BBC.

10.9 Taking employee details outside the BBC

All information relating to individuals e.g. electronic files such as lists of staff in spreadsheet format, personnel files, paper lists of salaries and staff appraisals, is covered by the DPA and the rules in this Handbook. In some circumstances BBC People staff or managers may have a legitimate reason to take employee information outside the BBC.

Examples of legitimate reasons to take information off-site

- Home working
- HR Managers taking personnel files to a case meeting in another building
- 24/7 staff taking home files to deal with out of hours emergencies

When taking personal information off-site, the following precautions should be followed:

- Electronic files should be encrypted in accordance with instructions from the Service Desk (02 26333)
- Files/documents/laptops etc should not be left on view in unattended vehicles
- Confidential papers/on screens should not be read on public transport/in public areas

- Files/documents/laptops should be kept under close personal control as far as reasonably practical.
- CDs/disks/laptops should not be identifiable as belonging to the BBC
- Laptops should not contain databases, spreadsheets or other large amounts of personal data on the hard drive unless they are encrypted. Please contact the IPC Team for advice on whether encryption is appropriate. Once a need for laptop encryption has been established, contact the Technology Service Desk (02 26333) to arrange for encryption software to be installed
- If, for practical reasons, personal information is processed on non-BBC PCs (e.g. writing up meeting notes at home), they should not normally be saved to the hard disk. The floppy disk/CD/memory stick used should be treated in the same way as any BBC disk - i.e. securely held while required and then destroyed.
- It is not normally acceptable to email personal details outside the BBC Network. However, you should apply your common sense since you can obviously email personal contact details outside the BBC in a work context.
- There are additional restrictions if you take or transfer information outside the European Activity Area. Please contact your DP Representative or the IPC Team for advice

Recording what personal information is taken off-site

- All files/documents should be booked out using an agreed procedure
- This procedure will vary from team to team and should be appropriate for the type of work and need not be excessive. For example, where a file is already booked out to an individual (as would be the case with a legacy hard copy personal file) no further booking out is needed as it is clearly recorded that the particular individual is responsible for its safe keeping. Where particular files are taken off site on a routine basis, it would be sufficient, for example, to tick a grid or make a diary note that this month's file has been taken.
- As a general rule all staff below grade 7 must obtain authorisation from a team leader or above to remove a file from BBC premises.
- The line manager must know at all times where all files are held
- Wherever possible files should be accessed electronically via myConnect desktop, and NOT downloaded to external computers.

NB there is no need (from a data protection perspective) to book out files that do not include personal data.

Returning materials

- All files/documents must be booked back in
- Logging systems must be checked by the line manager when a person leaves/moves to a different job to ensure all files/documents have been returned by that person

Regular home working

Where staff in a team regularly work at home, it may be appropriate for the manager to draw up additional guidelines/interpretations of this policy that relate to the precise tasks and work patterns of that team.

What to do if information is lost

Any employee personal information that is lost or stolen off-site should be reported immediately to the BBC People DP Representative who will trigger the Data Security Breach Procedures described in Module 15.

***Warning*: Failure to abide by this policy may result in disciplinary action.**

Module 11 - Marketing

SUMMARY

When you want to send marketing to individuals you must

- Obtain their consent before sending them marketing
- Provide a Privacy Notice informing individuals how the BBC will use their information
- Always provide individuals with an easy means of opting out of receiving marketing information
- Always suppress the details of individuals who have objected to receiving marketing
- Not use their personal information for a different purpose without obtaining their consent

Where we send information to BBC users about what services and programmes we provide, we are providing marketing. Direct marketing includes any promotional material you send directly to an individual using their personal information (e.g. email or postal address or text messages). At the BBC, we frequently use email newsletters about our programmes as a method of direct marketing. Even if the BBC is not commercially selling a product or service, the activity may still be marketing.

When we market directly to BBC users via email, phone, fax or text we are subject not only to the DPA but also to rules set down in the Privacy and Electronic Communications (EC Directive) Regulations 2003.

You should remember Rule 15 and Rule 16 when considering how the BBC may use personal information in order to send marketing.

11.1. Opt in/ Opt out

Opt-in is the mechanism by which an individual actively consents to the use of their personal information. You can obtain an individual's opt in consent through using a tick box, which should not be pre-ticked, which the individual should then tick if they agree to the use of their information. If the individual does tick an opt-in box, they are giving consent for their personal information to be used in the manner described.

Opt-out is the mechanism where the individual is already effectively opted-in to receive marketing and they need to actively indicate that they wish to opt-out. For example, a box could be pre-ticked and the individual should be informed that they need to un-tick the box if they wish to opt-out of receiving marketing.

Generally speaking, apart from certain areas of BBC Worldwide and the BBC Shop the BBC must operate on an **opt-in basis** under the Regulations.

11.2 Sending newsletters, e-newsletters and texts/ SMS

Email newsletters and text alerts can be great ways to keep our audience up to date with our programmes and other output. When we want to send a newsletter/alert or update about our programmes and services to our audience members we need to ensure the following:

- Individuals must positively consent to receiving the email or text
- We must only collect the minimum information needed from each individual - e.g. just their email address or phone number if that's all we need see also special considerations for children's data in Module 5.
- Include a proper Privacy notice when you're collecting the information explaining to the individual how we will use their information
- Always provide individuals with an unsubscribe notice
- Only use the personal information to send them that specific marketing communication
- If you no longer require the personal information (e.g. the individual unsubscribes from the newsletter) you should securely dispose of the personal information

If additional information is needed for a secondary purpose (e.g. gender, age etc. to provide effective personalisation of the marketing or service) then this information should be collected on an opt-in basis. A tick box opt-in or non-mandatory fields in an online form are both acceptable, but you must provide a clear explanation of what the information will be used for in all cases.

It is normally acceptable to add an invitation to an additional or related service to marketing communications (e.g. a link to a website collecting an audience for a live recording of a programme mentioned in a newsletter). However, this must clearly be on an opt-in basis only (e.g. the original email list for the programme newsletter cannot be used to advertise the live show, unless this purpose was made clear in the original opt-in and terms and conditions.)

The general test should be to consider what would be in the reasonable expectations of the individuals when they provided their personal details to the BBC.

11.3 Marketing - Unsubscribing from Marketing

An individual is entitled by written notice to ask the BBC to stop using their personal information for the purposes of direct marketing. This is otherwise known as 'opting out' or 'unsubscribing'. We must include an "Unsubscribe Notice" on each of our direct marketing materials giving individuals an opportunity, each time they receive a marketing message, to opt out.

If you receive a request from an individual to opt out of certain marketing, then you must stop using their personal details for that marketing communication within 28 days. You must also ensure that the BBC does not send them that marketing communication again unless they opt-in in the future. i.e. put their details on a 'suppression list' to ensure that they will not be targeted again in the future.

Please be aware that a failure to stop using their personal details may result in a court order being imposed against the BBC and disciplinary action against you. You should consider whether to acknowledge a request to opt out received from an individual, particularly if there is any

marketing in the pipeline which the individual may receive that cannot be prevented. You may wish to warn the individual in advance that they will receive this marketing but that their details will be suppressed as soon as possible.

Unsubscribe notice

In every single communication (each email or text etc) you must provide the individual with a simple means of unsubscribing from receiving the marketing. This should be free (except for the cost of transmission). The means provided should be suitable to the type of marketing. So, for an individual to unsubscribe from email marketing, unsubscribing should be via an email. To unsubscribe from text marketing should be via a return text (e.g. "Unsubscribe by texting "STOP" to 65555).

When you receive a request from an individual to unsubscribe from a marketing communication you must do the following:

- Act on the request as soon as possible (and in any event no later than 28 days after receiving the request)
- Remove all details of the individual EXCEPT any details you should keep on a "Suppression List"
- Maintain an accurate "Suppression List" which is a list of people who have requested that they be unsubscribed
- You must check against this list to ensure that no marketing is sent to individuals who have unsubscribed
- Only use the information for one purpose
- Securely dispose of the information (include suppression lists) once the service or marketing communication is finished

Module 12 - CCTV and Access Control Data

SUMMARY

In using CCTV at the BBC you must

- Understand that use of CCTV is limited to specific purposes
- Conduct an assessment before putting in place a CCTV scheme
- Have in place appropriate CCTV signage for schemes
- Respond to requests from individuals for copies of CCTV images

12.1 CCTV and the Data Protection Act

Most CCTV is directed at viewing and/or recording the activities of individuals. This means that the use of CCTV will need to be compliant with the DPA and the Information Commissioner's CCTV Code of Practice.

Using CCTV can intrude on the privacy of the people it captures, and as such, should only be used in limited circumstances.

12.2 The BBC's Use of CCTV Footage

The main use of CCTV is for monitoring the perimeter of BBC buildings.

If an incident is captured on CCTV (such as a theft, assault, accident, disturbance or trespasser), the operators of the CCTV may follow the progress of the incident, including any people involved.

Similarly, if an incident is later reported which may have been captured by CCTV, the BBC may review any footage of the incident captured by the cameras.

12.3 Access Control Data

Every time a BBC pass holder swipes their card for entry into BBC buildings this information is recorded. This is personal data as the information sets tells us about the buildings visited and the times of these visits. Therefore, as with all personal data Access Control Data must be appropriately processed.

12.4 Dealing with requests for CCTV footage and Access Control Data

The BBC receives requests from Individuals and Third Parties for access to CCTV footage and Access Control Data, which can be received through various parts of the BBC. Access Control Data is data held on the BBC's Access Control Management System and records the use of BBC identity cards to access buildings.

In order to ensure that these requests are dealt with consistently there are three BBC departments and two individual staff roles who are empowered to seek release of CCTV and Access Control data from the custodian of the information (the current contracted Service Partner). These are:

- Information Policy & Compliance
- BBC Investigation Services
- BBC Insurance Services
- Head of Information Security [1]
- Head of Corporate Security [2]

There are four general categories of requester for such data which are outlined in further detail below:

- Individuals (Subject Access Request).
- Police / Other Government Agencies
- Insurance Claim Representatives (contracted by the BBC)
- Third parties (such as Insurers/ Solicitors not related to the data subject)

12.4.1 Individuals (Subject Access Request)

Individuals (and their properly appointed representatives eg their solicitors or insurance agencies) have a right to request access to a copy of their personal information under section 7 of the Data Protection Act 1998, as it appears in CCTV footage. Individuals who require access to CCTV footage in which they appear must make a formal subject access request in writing to the Data Protection Office (see Module 14 for more information on dealing with SARs. This also includes where another person (e.g. friend, solicitor, insurer) makes a request for CCTV footage on behalf of the data subject.

Process

1. If you receive a request from a person for CCTV footage please advise the person to submit a request to:

   Data Protection Officer (Head of IPC)
   Room 2252
   White City
   201 Wood Lane
   London
   W12 7TS

   Or send an email to dpa.officer@bbc.co.uk

   You should advise the person that we will need the following information in order to deal with the request:

   - Date, time and address of the incident.
   - Copies of two pieces of identification - at least one of which includes a photo to allow the BBC to clearly recognise the applicant; this may be a driving licence, birth certificate, passport, rent book or utilities bill.
   - If a person is making a request on behalf of the data subject, they will also need to provide evidence that they have the data subject's consent to act on their behalf.

   - A further recent photograph of the requester in order that they can be identified in the footage requested. (Although this is not necessary when the footage required is of damage to the person's property, e.g. an accident in a BBC car park in which case the link between the individual and the property will have to be provided).
   - A £10 cheque made out to the BBC for subject access request fee.
   - A copy of the registration documents if the individual requires footage of his/her vehicle.

2. If you receive an initial request for CCTV footage make a record of it and contact the authorised person within Facilities Management [3] to require retention of the relevant footage, pending receipt of the formal request. Please also advise the IPC Team of the request and any details of the requester and action taken to date.

3. As soon as Facilities Management become aware of a request for CCTV footage it is the responsibility of the authorised person within Facilities Management to ensure the secure retention of the data if it exists, in an appropriate format for later assessment of disclosure.

4. Once the formal request has been received by IPC, along with the necessary details and payment, IPC will advise the person that the BBC has 40 days within which to respond to the request. IPC will also confirm the details with Facilities Management including whether or not CCTV data is available.

5. The BBC Investigation Service, having concluded that the application before them is justified, will request from the authorised person within Facilities Management, the release to them of the relevant footage. On request from the BBC, the authorised person within Facilities Management will ensure the safe provision of the CCTV data in accordance with the agreed process and format.

6. If it is decided that disclosure is justified then the authorised person in Facilities Management should be advised that the data shall be retained to enable disclosure. If it is decided that disclosure is not justified then the authorised person in Facilities Management should be advised to retain the data as normal. Facilities Management will only destroy the data after authorisation from the department giving the original instruction on retention.

12.4.2 Police / Other Government Agencies

Requests from the Police and other government agencies are dealt with by the BBC Investigation Services.

Process

1. If you receive a request for CCTV footage/access control data from the Police or any other government agencies, please advise Facilities Management or BBC Investigation Services.

2. Facilities Management may release footage to the Police as part of enquiries into a crime unconnected with BBC staff, Service Partners or Visitors. This must only be done where Facilities Management are satisfied that failure to provide the footage would be likely to prejudice either:

   - the prevention or detection of crime or
   - apprehension/prosecution of offenders

Facilities Management keep adequate records in order to produce evidence for how they reached the decision to release the footage. Facilities Management contact BBC Investigations with any questions.

3. Where an investigation relates to BBC staff, Service Partners or Visitors BBC Investigation Services may release CCTV or access control data where they are satisfied that failure to provide the footage would be likely to prejudice either:

    - the prevention or detection of crime or
    - apprehension/prosecution of offenders

    BBC Investigations keep adequate records in order to produce evidence for how they reached the decision to release the footage.

4. Where other parties request CCTV footage BBC Investigations will require the completion of a Section 29 DPA 1998 Request form and that they make a formal application to:

    Room 1534
    BBC White City
    201 Wood Lane
    London
    W12 7TS

    Or

    Fax: 020 875 24213

    The form requires the requester to set out the exemption under the DPA and justification for lawful disclosure.

5. The BBC Investigation Service will be responsible for the review and validation of the request to ensure disclosure is reasonable, necessary, proportionate in all circumstances, and justified.

12.4.3 Insurance Claim Representatives (Contracted by the BBC)

If the request for CCTV footage relates to a BBC Insurance claim they will need to make an application for the data via BBC Insurance Services.

BBC Insurance Services will be responsible for the review and validation of the request to ensure disclosure is reasonable, necessary, proportionate in all the circumstances, and justified.

12.4.4 Requests by third parties and under Freedom of Information

Updated June 2009

If people are capable of being identified in CCTV images then this is personal information. This information can most likely NOT be disclosed in response to a Freedom of Information request [4].

However, it will appropriate to release images to a third party where their needs outweigh those of the individuals whose images are recorded.

Requests from insurance companies for CCTV of damage to their client's property can be dealt with by Facilities Management. In order to disclose footage to an insurance company the form CCTV Data Request Form (for property damage on BBC premises) must be completed by the insurance company and submitted to the person responsible [5] for viewing, management and/or downloading (i.e. processing) of CCTV data.

If the application is reasonable and justified then viewing of the specific incident may take place and be downloaded if necessary for the business purpose. The transaction will also be recorded on the Facilities Management Incident / Download Form and dealt with in accordance with established practice.

The completed CCTV Data Request Form will be forwarded to the BBC Workplace contact [6] who will monitor DPA compliance.

In the case of request from other third parties for CCTV, BBC Investigations, BBC Insurance or IPC will be able to decide whether the CCTV data is released.

They will ensure the following:

- The requests are genuine (they will investigate why the data is being sought and confirm this to their satisfaction;
- the footage will only be used for a specified purpose (eg insurance claim); and
- there is no risk to the safety of other people involved (eg it would not be appropriate to release data of an adulterous couple kissing in the carpark to one of their spouses)

If you have any queries about whether the footage should be given out, please contact IPC for further advice.

12.5 Deciding whether to use CCTV or continue using CCTV

Pursuant to the Information Commissioner's guidance on appropriate deployment and use of CCTV the BBC has the following policies on deciding when to use CCTV and appropriate signage.

The BBC uses CCTV to provide a safe and secure environment for BBC employees, audiences and other visitors. Currently, the BBC has in place perimeter security CCTV systems as part of a range of security measures derived from the Building Security Risk Assessment (BSRA) carried out for all of its buildings. The assessment is carried out by either the Head of Corporate Security, or third parties engaged by BBC Workplace, or its Facilities Management Providers.

During these assessments the BBC needs to carefully consider whether the installation of CCTV is necessary. We need to take into account what benefits can be gained, whether better solutions exist and what effect it may have on individuals.

Key issues to consider when using CCTV are:

- What organisation will be processing the CCTV images - will it be BBC staff or external contractors?
- If it is external contractors, do we have a contract in place which includes data protection clauses?
- What is the BBC's purpose for using CCTV? What problems is it meant to address?
- What are the benefits to be gained from its use?
- Can a less privacy-intrusive solution, such as improved lighting, achieve the same objectives?

- Does the BBC need images of identifiable individuals, or could the CCTV use a system where images are not capable of identifying individuals?
- What future demands may arise for wider use of images and how will the BBC address these?
- What could the BBC do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?
- What CCTV product will be used and does it capture images of a sufficient quality to meet the proposed objectives
- Where should cameras be sited (both to ensure adequate coverage to meet the objectives of the scheme and to minimise collateral intrusions.

Corporate Security monitors the BSRAs and periodically review them.

12.6 CCTV Signage

Where a CCTV scheme is to be installed/in operation, to comply with the 1st principle of data protection people must know that they are in an area where CCTV surveillance is being carried out.

The most effective way of doing this is by using prominently placed signs at the entrance to the CCTV zone and reinforcing this with further signs inside the area.

CCTV signage should:

- be clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using CCTV and who to contact about the scheme (where these things are not obvious to those being monitored); and
- be an appropriate size depending on context, for example, whether they are viewed by pedestrians or car drivers.

---

[1] Currently Julia Harris

[2] Currently Eddie Halling

[3] Currently Richard Jowsey or Tim Cavanagh in BBC Workplace for London, Scotland and English Regions, Bill Smale for Wales and Roisin Brown for Northern Ireland

[4] As set out in CCTV Code of Practice p17

[5] Currently Robert Kennedy, BBC Workplace for London & Scotland and Mick Taylor, BBC Workplace for English Regions

[6] Currently Kate Hodson, BBC Workplace

Module 13 - Programme Making and Data Protection

1. BBC's role as a programme maker

The BBC as a broadcaster collects and uses huge amounts of personal information for a variety of programme-related reasons, such as in news stories and through user generated content on our websites.

While this personal information is subject to the DPA and its requirements, in recognition of the unique role of the media in relation to freedom of expression, there are some limited circumstances in which the BBC is exempt from complying with some provisions of the Act.

The specific exemption is outlined in section 32 of the DPA and applies to personal information which is processed for the purposes of journalism and/or art and/or literature. It is important to bear in mind that this is not a blanket exemption for the BBC and has to be considered carefully in each specific case where we need to rely on it.

2. The scope of the exemption

Three conditions MUST be fulfilled if S32 is to be invoked:

- *Process data with a view to publishing journalistic or artistic material; AND*
- *Publication is in the public interest (this decision is based on whether a programme is made in accordance with the BBC Editorial Guidelines); AND*
- *It would be **incompatible** with our journalism to comply with the data protection provisions*

1. The processing of the personal data is undertaken with a view to publishing journalistic, literary or artistic material

The BBC views this first provision as relatively wide and processing will capture most things done with personal information such as:

- Obtaining it
- Recording it
- Holding it
- Operations such as; organising it, altering it, retrieving it, using it, disclosing it etc.

You will also need to be carrying out one of the above actions with the view to publishing journalistic, artistic or literary material.

While the application of the exemption will need to be made on a case by case basis, one interpretation of the requirement is that you are carrying out one of the above actions on the personal information with the intention or hope of publishing material, such as programme content.

The Information Commissioner has also defined 'publishing' in the DPA to mean that the information is made available to the public or any section of the public.

2. We have had regard to the special importance of the public interest in freedom of expression and reasonably believe publication would be in the public interest; and

This provision requires the BBC to complete a public interest balancing test to determine whether it would be in the public interest to publish the material in question.

While the application of the exemption will need to be made on a case by case basis, if you are able to process the personal information in compliance with the BBC's Editorial Guidelines, it will usually be a good indicator that the publication is in the public interest.

3. We reasonably believe in all the circumstances that compliance with the specific provisions of the DPA is incompatible with journalism and/or artistic purposes and/or literary purposes.

The third provision requires the BBC to show that we reasonably believe we cannot apply the provisions of the Data Protection Act as well as maintaining the journalistic purposes etc for which we collected the personal information. It is not enough just to show that it would be inconvenient to comply, you must be able to show that it would be incompatible to do so.

For example, if we had a story about a corrupt MP and the MP made a request under section 10 of the DPA to prevent us using his personal information in the story, we would be unable to do our job as a broadcaster and inform the public know of an important issue. In these circumstances, we could not comply with the Data Protection Act as well as continue with the story.

3. How the exemption works

This exemption is similar to the derogation provided in the Freedom of Information Act, 'journalism', 'art' and 'literature' and is usually taken to mean our content, or activities closely associated with content creation. It includes our online content.

The specific provisions of the DPA which we would not need to comply with when relying on the exemption, and incompatibility can be shown, are:

- The data protection principles, except for the seventh data protection principle, which relates to the security of the data.
- If an individual tried to exercise their rights under the Data Protection Act, namely:
    a. Subject Access Requests (section 7)
    b. Preventing processing likely to cause damage or distress to the data subject upon their request (section 10)
    c. Providing rights to the data subject in relation to automatic decision making (section 12); and
    d. Rectification, blocking, erasure and destruction of the personal information (section 14(1) to (3)).

Although we would not have to comply with most of the data protection principles if we relied on the exemption, we would still have to comply with the 7th data protection principle, which relates to keeping personal information secure.

This means when you collect the information you will still need to ensure that you keep the information secure, such as locking away any hard copy information and laptops when they're not in use and keeping electronic information password protected. You also need to ensure that only those people who have a business need have access to the information. For further information see Module 9 - Security and Deletion of Personal Information and the BBC's Information Security Policies.

Note also that the exemption has specific provisions to protect the media against court action before material is published. If you become aware of any threatened use of the Data Protection Act before your material is due to be broadcast or put online, you should immediately contact IPC, who will liaise with the Litigation Department.

4. What can the ICO do?

The ICO has specific powers when dealing with personal data processed under section 32. If the ICO believes that we are not processing the personal data only for the special purposes, or are not processing it with a view to publication, he can issue a special enforcement notice on us. Any failure by the BBC to comply with an enforcement notice is an offence.

The reputational risk to the BBC of such an action by the ICO would clearly be very serious.

6. Further help

Application of this exemption can be complex. If you need any further help about using the exemption please contact the IPC Team.

Module 14 - Subject Access Requests

SUMMARY

Individuals have the right to ask for a copy of their personal information that the BBC holds. Please note that

- You need to be able to recognise a SAR
- When you receive a SAR you must contact the IPC Team immediately as there is a specific legal timeframe to respond to requests
- You may be asked to search for information on your systems by the IPC Team in response to a SAR

The DPA gives living individuals the right to request access to records and other information that organisations hold about them. This is called a Subject Access Request or "SAR". Except where exemptions apply, in response to a request, the BBC must provide to individuals copies of all records and information that it holds on that individual in response to a SAR.

Please be aware that the BBC has *40 days* within which to respond to a SAR. Failure to respond within the 40 day specified time limit is a breach of the DPA by the BBC. Therefore, it is imperative that requests are forwarded on immediately to IPC so work can commence.

Under this right, an individual is entitled to a copy of his or her own personal information subject to a number of exemptions. Furthermore, an individual may not be entitled to information relating to third parties (particularly, where information has been provided in confidence).

14.1 How do I recognise a Subject Access Request?

The BBC regards any request for a large amount of personal information as a SAR. Please note that it must be for personal information *about* the person who is actually making the request (although bear in mind that an individual may make a request through his or her solicitor). Otherwise it may be a request for personal information about another person under the Freedom of Information Act 2000.

E.g.: *Can you please provide me a copy of all the information the BBC holds about me?* or *Can you provide a copy of all my personnel records from 1997 - 2007.*

With respect to the first example request above, generally we would ask the requestor to give more information about the personal information they are requesting to help us locate that information. By way of general guidance, business as usual requests for discrete pieces of information should NOT be treated as a SAR. However, this is a judgment that you will need to make and IPC will be able to help you with this if need be.

So a request such as *"Can you please provide a copy of my appraisal from last year?"* is really a business as usual request and does not need to be treated as a SAR.

However, if there is a reason why personal information is NOT going to be released in the course of business as usual, then the request must be treated as a SAR and should be referred to the IPC.

14.2 What do I do with a SAR?

You must immediately pass a SAR (or anything that *might* be a SAR) to the IPC Team, at Room 2252, White City, 201 Wood Lane, London, W12 7TS or forward via email to DP Advice.

14.3 How long have we got to respond to a SAR?

The BBC has 40 calendar days to respond to a SAR from the day upon which the BBC has received all the necessary information about identity, location of the information and the fee (if relevant). However, where the request is provided with all the necessary information and the fee, the 40 calendar days will start to run *on the day that the request is received* (regardless of who within the BBC receives it). Given the considerable amount of work involved in responding to SARs and the short timeframe it is important that you pass any SAR immediately to the IPC Team.

14.4 ID requirements and payment

The BBC will also require 2 forms of identification to ensure that the requester is who they claim to be. At least one of which should be photographic, and the other should preferably confirm address. Identification is important since we need to ensure that personal information is provided to the person to whom it relates rather than any other person.

A SAR will attract a £10 fee which is payable to the BBC via postal order or cheque made out to the BBC.

14.5 What should the BBC provide to a requester?

In response to a SAR, a requester is entitled to be informed:

- whether the BBC holds any personal information about them
- to be given a description of the information
- to be told for what purposes the information is used
- to be given a description of the recipients or the classes of recipients to whom the information has been or may be disclosed (e.g. an independent production company, or BBC's outsource service providers for employees)

The requester is also entitled to receive:

- a copy of the personal information with any unintelligible terms explained
- any information available to the BBC about the source of the personal information

- an explanation as to how any automated decisions taken about them have been made
- and, if the requester has specifically requested it, to be informed of the logic involved in any automated decisions.

14.7 What personal information can be withheld by the BBC?

The BBC may not be able to release personal information in response to a SAR where it falls under an exemption such as being personal information relating to other people. Other exemptions include where information is used for crime prevention and detection or is covered by legal professional privilege.

However, please note that decisions about the use of these exemptions must be made by the IPC team.

If you have any questions about SARs please contact the IPC team.

14.8 How do I search for information?

When you are requested to provide information in response to a SAR you must search **all paper and electronic documents (including emails)** that you hold. However, if you have questions about the extent of your search, for example, you believe that it would be very time consuming, please contact the IPC team (the general test in this case is that if you could find the data if you needed it for your own purposes, then you should disclose it for the purpose of an SAR).

You are required to search the following types of records:

1. Information held electronically, including emails and Word, Excel or other electronic documents. With respect to emails, you must search your 'inbox', 'sent items' and 'deleted items' folders. You do not have to search permanently deleted items which only IT support could retrieve for you;

2. CD Roms and disks; and

3. Information held in paper files, including handwritten notes and other hard copy documents. You must search paper files that are structured by reference to individuals (e.g. alphabetical index or unique identifier) and unstructured (administrative or miscellaneous files with information held chronologically).

14.9 I have found some embarrassing emails - do I have to disclose these?

Yes, you do. Please note that it may be a criminal offence under the FOIA and/ or the DPA to alter, deface, block, erase, destroy or conceal any record held by the BBC with the intention of preventing its disclosure.

14.10 What happens after I've located the information?

Please provide the relevant information to the IPC Team, who will go through the information you have provided and assess whether any exemptions apply. Information that is exempt will be

removed, or redacted from documents, and the remaining information will be sent to the requester.

Module 15 - Data Security Breaches

Data Security Breach Procedures

Data security breaches can have a massive impact on individuals associated with the BBC as well as the reputation and efficiency of the BBC. This procedure sets out the actions that you must take immediately upon becoming aware of a data security breach.

15.1 What is a data security breach?

Loss/disclosure/inappropriate access or mishandling of either:

- Large volumes of personal data (i.e. details of more than 100 individuals)
- Personal data that that could cause potential harm to the individuals (e.g. financial/credit card details for a small number of staff); or
- Particularly sensitive data for smaller volumes (e.g. medical records, contract details of key talent, contact details of anonymous sources).

If in doubt about whether an event is a data security breach - contact IPC immediately on 02 26599.

15.2 What to do in the event of a data security breach?

1. Inform your DP Representative* immediately and appropriate DP Contact. Who is my DP Representative?
2. DP Representative will then assess whether event is significant enough to qualify as a "Serious Incident". If so s/he will contact IPC immediately on mobile numbers as set out in contact list below.
3. IPC to alert DP Serious Incident Group
4. Division to provide Relevant Information (see Procedures for DP Serious Incident Group) within 4 hours of report of Serious Incident
5. If DP Representative assesses the event to be minor s/he should notify IPC via email "Data Protection Advice" within 24 hours of report.
6. Where the data security breach involves personal data lost as a result of theft or thefts/loss of portable devices (laptops/PDAs) including personal data report this to BBC Investigations.

*Note, DP Representatives will need to arrange for cover for this function for sickness/leave, and ensure that their Departmental Data Protection Contacts know of the arrangements.

15.3 What will happen then?

A group of senior people will form the DP Serious Incident Group and will gather the Relevant Information and decide how to act on the breach.

15.4 Procedures for DP Serious Incident Group

These procedures are additional to the Data Security Breach Procedures and set out how serious data protection breaches will be managed within the BBC once a breach is reported.

DP Serious Incident Group to meet to decide how breach should be acted upon. The DP Serious Incident Group is comprised of:

a. DP Serious Incident Group - Core Group

1. Chief Operating Officer
2. Relevant Divisional Director
3. General Counsel
4. Head of Press Office
5. Head of Information Policy and Compliance

b. DP Serious Incident Group - members as necessary

Other staff will be invited to join the group depending upon the nature of the incident. For example:

- Director of BBC People (e.g. incidents involving significant numbers of staff)
- Director of Vision/ Audio & Music (As appropriate) (e.g. cases involving talent)
- Channel/Network Controller (As appropriate)
- Head of Rights and Business Affairs (e.g. cases involving talent)
- Directors General's Office

c. Additional support and external contact

A number of staff may be called upon to provide expert advice to the escalation group for example:

- Head of Investigations Unit
- Head of Internal Communications
- Head of Business Continuity
- Head of Employment Law
- Head of Information Security

As the information about an incident is confirmed the Escalation Group may decide to inform representatives from such bodies as:

- The BBC Trust
- The Information Commissioner's Office
- The Police
- Outsource Company Press Office (if appropriate)

d. Deputising

When Head of Information Policy and compliance is away his deputy will be the IPC Senior Adviser, Policy. They will be responsible for ensuring that appropriate deputies were contacted where members of the core incident escalation group are unavailable.

15.5 Relevant Information to provide to Serious Escalation Group

The Division must inform the Serious Escalation Group of the following within 4 hours of report (IPC can also provide assistance where necessary):

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
- Is a crime suspected? Have the police been notified?
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, audience members or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

15.6 Freedom of Information

Please note that all documents that are created by the DP Serious Incident Group may be disclosable under FOI unless a suitable exemption applies (e.g. legal professional privilege). Please speak to IPC with any questions on this matter.

USEFUL CONTACTS

James Leaton Gray
Head of Information Policy and Compliance

james.leaton.gray@bbc.co.uk
Internal Number: 02 26567
Mobile number: 07740 818 036

Lucy McGrath
Senior Adviser, Policy, Information Policy & Compliance

lucy.mcgrath@bbc.co.uk
Internal Number: 02 26647
Mobile Number: 07809 597 645

Module 16 - Complaints about Breaches of the Data Protection Act

SUMMARY

Individuals have the right to complain to the BBC about the way their personal information is used (see Rule 11). We must ensure that we treat these complaints properly and in accordance with this Handbook. In particular

- Individuals may claim that the way that the BBC uses their personal information causes them damage or distress

16.1 An individual claims that use of their personal information is causing damage or distress (section 10 notice)

Individuals may provide a written notice to the BBC that the use that we are making of their personal information is causing them damage or distress and request that we stop using or not begin to use their information. This is officially called a section 10 notice under the DPA. When the BBC receives a section 10 notice, it has 21 days within which to reply to the individual so it is important that you contact the IPC team directly.

If this complaint is in relation to a news item, message board or other broadcast or web item, do not take any action without consulting the IPC Team or Programme Legal Advice.

You should be aware that an individual who suffers damage, or damage and distress, as a result of any contravention of the requirements of the DPA by the BBC has a right to claim compensation from the BBC. However, the damage or distress must be substantial and unwarranted.

Please contact the IPC team for further guidance. However, you should be aware that the DPA sometimes permits the BBC to use personal information for the purposes of journalism, literature and art regardless of whether substantial distress or damage is caused. See Module 13 for more information about journalism and the DPA.

16.2 The BBC receives a request to remove User Generated Content

As we provide the ability for users to post content onto the BBC website or our associated websites, we may from time to time receive content from individuals which includes personal information on another third party individual e.g. where John provides comments on a BBC website about Peter without Peter's knowledge or permission. Where this occurs, the third party individual may contact the BBC to ask that the BBC remove this content.

The third party individual may also object to content being posted about them on a BBC website because the comments are defamatory. You should be aware that the BBC could be subject to an action for defamation. Please contact Programme Legal Advice for further advice on defamation.

16.3 Rectification, blocking, erasure and destruction of inaccurate data

Where an individual has made a SAR and has received a copy of their personal information they may consider that the information is not accurate or should be deleted. The individuals may then contact the BBC to ask that the information be rectified.

If the BBC disagrees, the individual may then take the matter before the court to obtain an order to force the BBC to change or delete the information.

If you receive a notice in writing requesting rectification of the information due to its inaccuracy, contact the IPC Team or email Data Protection Advice for advice. In particular it is essential to seek advice from the IPC Team or Programme Legal Advice where the request relates to BBC's broadcast or online content. This is because there are different laws relating to broadcast material and, as a consequence sometimes these rights will not be available to individuals.

16.4 Other complaints

Should you receive any other complaints from individuals about the way the BBC uses their personal information, please contact the IPC team for advice.

Module 17 - Encryption of BBC Data

17. Personal Data

In order to protect personal data Information Policy and Compliance have defined rules for personal data which must be encrypted. This requirement applies to all personal data collected for the BBC, even if held by Independent or 3rd party organisations.

17.1 What personal data should be encrypted?

- All documents holding sensitive data relating to named individuals where the distress that might result from the misuse or disclosure would be deemed significant (e.g. major talent salaries, medical conditions ethnicity, religious or information about sex life)
- All Children's contact details
- Documents holding named information and their financial information (bank details etc) of more than 50 individuals.
- All documents holding names and other non-sensitive personal data (e.g. date of birth or National Insurance Number) of more than 1,000 individuals.

17.2 Other Data

Individual department or Divisions can define additional types or groups of data that should be encrypted. The processes will be the same as those defined below.

17.3 How should I encrypt data?

17.3.1 *Data being sent via e-mail*

Regular third parties in receipt of BBC encrypted data

Where the BBC has a regular communication with 3rd parties, an encrypted tunnel will be created between the BBC and the 3rd party. This means that the user need perform no further action, their mail will automatically be encrypted between the BBC and its destination.

Current encrypted tunnels exist between the BBC and

- Capita HR Direct
- Red Bee Media (RBM)

Other 3rd parties

The BBC currently only provides encryption through usage of WinZip. This means that the document has to be added to a WinZip file, and a password applied. This password must not be sent with the document in question, but communicated via telephone. Instructions for how to perform this function can be found on the BBC IS website here

If the third party is sending a WinZip file to the BBC, it must be zipped using WinZip V9.0 or higher, the encryption below this version of WinZip is not strong enough.

If you need to find out what version of WinZip is running, open WinZip, and under the Help menu is About WinZip, this displays various information including the version number.

17.3.2 *Data being sent via means other than e-mail*

Encrypted memory stick

The BBC recommends usage of a encrypted memory stick, which are available to buy on Quick Order. Again the password must not be stored with the stick itself. However if any other device is available, please check with ism@bbc.co.uk to ensure that the encryption used is suitable to protect BBC data.

CD Rom or DVD

The data should be saved to the CD Rom/DVD in the form of a WinZip file, instructions above.

17.4 How do I decrypt data?

If you have received data from a 3rd party that is encrypted, you need to follow their requirements. Please ensure you receive passwords by phone, or through the post, and not via the same route that the data has taken.

If it is a password encrypted WinZip file, entering the password as given by the third party will decrypt the data.

17.5 Can I encrypt portable data (e.g. Phones/PDAs/Blackberrys)?

Currently the BBC has no capability to encrypt data on these devices. It is requested that the manager of a department seriously consider if it is appropriate to use these devices if personal data is being transported. Advice should be sought from the department DPA Representative. A list of these can be found on the IPC website.

17.6 Laptop Encryption

The BBC is working on the capability of encrypting data on laptops.

This service should be available before Summer 2009.

Version control

Version	Date	Notes	Version approved by
V1	August 2008		Lucy McGrath
V2	June 2009	Changes – date on header page Addition to module 12.4.4 - CCTV requests from insurance companies	Lucy McGrath