BRENTWOOD BOROUGH COUNCIL

Data Protection Policy

1st Draft

Title:	Data Protection Policy
Purpose:	To ensure information is kept secure
Owner:	Data Protection Officer
Approved by:	Head of Legal Services
Date:	July 2017
Version No:	1.0
Status:	SUBJECT TO COMMITTEE APPROVAL
Review Frequency:	Annually or when changes made to relevant Information Governance law
Next review date:	As above
Meta Compliance	IT to ensure policy subject to this

Introduction

This policy defines the Data Protection Policy and is part of the Information Governance suite of policies currently under review. If you require advice and assistance around any Information Governance matters (including for example Data Protection, data security and FOI requests) please contact the council's Data Protection Officer (DPO). Further information and resources including training and other online support are available on the council's intranet at: [TBA - best practice would in due course see in place a dedicated, high-profile intranet page on FOI and DPA with contact details of the DPO, FOI/SAR co-ordinator and with links to helpful ICO guidance pages, online training tools and our related policies]

General rules in complying with the Data Protection Act

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. All BBC staff must comply with the requirements of the Data Protection Act and Article 8 of the Human Rights Act when handling personal data of living individuals; whether relating to members of the public or other BBC staff.

2. Staff who manage services where personal data is used must make sure that the service users are informed why we need their data and how we intend to use it. Their consent must be obtained and they must be made aware of their rights under the Data Protection Act.

3. All staff must collect, hold and use the minimum personal data necessary to deliver our services.

4. All staff who record opinions or intentions about service users must do so carefully and professionally.

5. All staff must take reasonable steps to ensure the data we hold is accurate, up to date and not misleading.

6. Consent must be obtained if personal data is to be used in ways not expected by the data subject, or different from the reasons the personal data was originally obtained for example, for promoting or marketing goods and services or under a new data sharing agreement.

7. All managers must ensure that the personal data they manage is reviewed regularly and destroyed in line with your retention and archiving requirements when no longer required.

8. If you receive a request from a member of the public or a member of BBC staff asking to access their personal information, you must pass this to the FOI/DPA Co-ordinator for logging and processing.

9. If you receive a request from anyone asking to access the personal information of **someone other than themselves**, this must be handled as a Freedom of Information Request or Environmental Information Regulations Request and in the first instance must be passed immediately to the FOI/DPA Co-ordinator for logging and processing.

10. If someone contacts BBC formally stating that their personal data on our records is inaccurate, the request should be fully considered and the record amended if the request is valid. Again, please ensure such requests are passed to the FOI/DPA Co-ordinator for logging and processing.

11. You must follow system user guidance or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so. If you suspect any system puts BBC in breach of this requirement, please immediately notify the Data Protection Officer.

12. Information must only be shared with external organisations if it is done under a formal Information Sharing Agreement which clearly explains the limits of what can be shared, why and what safeguards will be in place to protect individuals' personal data.

13. All staff and elected members must be trained to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely.

14. When using 'data matching' techniques, this must only be done for specific purposes in line with formal codes of practice, informing service users of the details and obtaining their consent where appropriate.

15. The Council must maintain an up to date entry in the Public Register of Data Controllers **(this requirement will cease under new Regulations being adopted on 25 May 2018).**

16. Where personal data needs to be anonymised or pseudonymised, for example for research purposes and you are uncertain how to proceed with this, please seek guidance from the Data Protection Officer and/or IT Services.

17. You must not access personal data which is not necessary for you to see unless it is required in order for you to do your job properly.

18. You must not share any personal data held by BBC with any individual or organisation based in any country outside of the European Economic Area (European Union member states and Iceland, Liechtenstein and Norway).

Why must I do it? (Note - please see list of the 8 Data Protection Principles further below)

1. To comply with UK legislation.

2. To comply with the 1st and 2nd Principles of the Data Protection Act.

3. To comply with the 2nd and 3rd Principles of the Data Protection Act. You must only collect and/or hold the minimum amount of information you need in order to carry out our legitimate business. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep information up to date may mean that information that was originally accurate becomes inaccurate.

4. To comply with the 3rd and 4th Principle of the Data Protection Act.

5. To comply with the 4th Principle of the Data Protection Act.

6. To comply with the 1st Principle of the Data Protection Act.

7. To comply with the 3rd and 5th Principle of the Data Protection Act. If information is kept longer than necessary then it may be both irrelevant and excessive.

8. To comply with the 6th Principle of the Data Protection Act.

9. To comply with the 1st Principle of the Data Protection Act, the Freedom of Information Act and the Environmental Information Regulations.

10. To comply with the 6th Principle of the Data Protection Act.

11. To comply with the 7th Principle of the Data Protection Act.

12. To comply with the 1st and 7th Principle of the Data Protection Act.

13. To comply with the 7th Principle of the Data Protection Act.

14. To comply with the 1st and 6th Principle of the Data Protection Act.

15. This is a regulatory requirement and allows the public to see what personal information we hold to aid transparency.

16. Where personal data is used for research purposes, the processing of the data can be legitimised by virtue of s33 Data Protection Act. Relevant guidance available from the Data Protection Officer.

17. To comply with the 7th Principle of the Data Protection Act.

18. To comply with the 8th Principle of the Data Protection Act. The member states of the EEA share common legislation which provides assurance to BBC that personal data will be handled securely under the same provisions that exist under the Data Protection Act.

How must I do it?

1. By following the requirements of this policy.

2. By following the requirements in the Privacy Notice Policy and the Consent Policy

3. By ensuring that the means you use to gather personal data (such as online or physical forms) only ask for the information that is required in order to deliver the service.

4. By considering that anything committed to record about an individual may be accessible by that individual in the future.

5. For example, whenever contact is re-established with a service user, you should check that the information you hold about them is still correct.

6. By following the points in the Privacy Notice Policy and the Consent Policy.

7. By following your Service's Retention and Archiving requirements. You must review personal data regularly and delete information which is no longer required, although you must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the Act allows us to keep indefinitely personal data processed only for historical, statistical or research purposes.

8. By ensuring that all requests for personal data or other information under FOI/EIR are immediately referred to the FOI/EIR Co-ordinator for initial consideration and in order to co-ordinate responses as required. This also includes requests to amend someone's personal data.

9. By immediately referring to the FOI/EIR Co-ordinator as referred to at 8. above.

10. By immediately referring to the FOI/EIR Co-ordinator as referred to at 8. above.

11. By being aware of the requirements of relevant I.T. policies and any other relevant policies in relation to:

- technical methods such as encryption, password protection of systems, restricting access to network folders
- physical measures such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure and
- organisational measures such as providing proper induction and training so that staff know what is expected of them.

12. Consult the FOI/DPA Co-ordinator over any proposed sharing outside of the EEA. If you are a manager who is proposing a change to or implementing a new system which may involve the hosting of personal data whether within or outside the EEA, this must first be tested using a Privacy Impact Assessment. See Privacy Impact Assessment Policy**.**

13. By completing training courses relevant to your role.

14. By consulting the Data Protection Officer and/or I.T. Services to establish whether the proposed process is appropriate.

15. Updates to be made when any change to the purposes of processing personal data occur (eg under a new Information Sharing Agreement).

16. Contact the Data Protection Officer for guidance if required.

17. By being aware through training and guidance from your manager on what information is appropriate for you to access to do your job.

18. Check with your line manager whether a relevant data sharing agreement is in place.

The Eight Data Protection Principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, check with the Data Protection Officer on how best to proceed.

If you believe the policy does not meet your business needs, you may raise this with the Data Protection Officer who may propose a policy change if appropriate.

References:

Data Protection Act 1998

Human Rights Act

Lawful Business Practice Regulations 2000

ICO: Employment Practices Code and Supplementary Guidance

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you. The Council as well as those individuals affected is also at risk of financial and reputational harm. Currently fines of up to £500,000 may be imposed on Councils for serious data breaches. Please report any actual or potential data breaches or other concerns relating to Information Governance to the Data Protection Officer as soon as possible.