Data Protection Policy Statement

Introduction

This policy defines Brentwood Borough Council's Data Protection Policy and is part of the Information Governance suite of policies adopted by the council. The council is committed to full compliance with the requirements of the General Data Protection Regulation and the Data Protection Act 2018. The council seeks to ensure that all employees, elected Members, contractors, consultants, partners or other servants or agents of the council who have access to any personal data held by or on behalf of the council are fully aware of and abide by their duties under the law.

Statement of Policy

The council needs to collect and use information about people with whom it works to operate and carry out its functions. These may include members of the public, current, past and prospective employees, clients and customers and suppliers. In addition, the council may be required by law to collect and use information to comply with the requirements of central government. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

Brentwood Borough Council regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the council and those with whom it carries out business.

Handling personal data

Brentwood Borough Council will, through management and use of appropriate controls, monitoring and review:

- Use personal data in the most efficient and effective way to deliver better services
- Strive to collect, process and retain only the data which is needed
- Use personal data for such purposes as are described at the point of collection, or for purposes which are legally permitted
- Strive to ensure information is accurate
- Not keep information for longer than is necessary
- Securely destroy data which is no longer needed
- Take appropriate technical and organisational security measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data)
- Ensure that information is not transferred abroad without suitable safeguards
- Ensure that there is general information made available to the public of their rights to access information
- Ensure that the legal **rights** of people about whom information is held can be fully exercised. These rights include:

    - ✓ The right to be informed
    - ✓ The right of access to personal information
    - ✓ The right to request rectification
    - ✓ The right to request erasure ("the right to be forgotten")
    - ✓ The right to restrict processing in certain circumstances
    - ✓ The right to data portability
    - ✓ The right to object to processing

The Principles of Data Protection

Anyone processing personal data must comply with 6 principles of good practice. These principles are legally enforceable.

Summarised, the principles require that personal data shall be:

1. processed lawfully, fairly and in a transparent manner
2.collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which is not incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods where it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures in accordance with the rights of data subjects under the GDPR/ Act

Definitions

The legislation provides conditions for the processing of any personal data and makes a distinction between personal data and 'special category' data.

Personal data is defined as any information relating to an identified or identifiable natural person

Special category data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious/philosophical beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life or sexual orientation
- Biometric data

APPENDIX – GUIDANCE TO STAFF

General rules in complying with the GDPR and Data Protection Act 2018

Definitions

The legislation comprising the GDPR and DPA provides conditions for the processing of any personal data.

Personal data is defined as any information relating to an identified or identifiable natural person

Special category data (previously known as "sensitive personal data") is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious/philosophical beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life or sexual orientation
- Biometric data

Special category data may only be processed if condition in Article 9 of the GDPR are met.

Data relating to **criminal offences** are treated separately from sensitive personal data. Criminal offence data may only be processed if conditions in Article 10 of the GDPR are met.

Data Protection Act means the Data Protection Act 2018

DPO means a Data Protection Officer

GDPR means Regulation (EU) 2016/679 (the General Data Protection Regulation).

Privacy Impact Assessment means a Data Protection Impact Assessment, which is a structured review of a processing activity from a data protection compliance perspective.

Controller means the person or body which determines the purposes and means of processing personal data.

Processing means any operation that is performed upon personal data and **Processor** means a person or entity that processes personal data on behalf of a controller.

Profiling means processing for the purposes of evaluating personal data in order to analyse or predict the behaviour of a data subject.

What must I do?

1. You must comply with the requirements of the GDPR, Data Protection Act and the Human Rights Act when handling personal data of living individuals, whether relating to members of the public or BBC staff/members
2. You 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 law
3. You must collect, hold and use the minimum personal data necessary to deliver our services.
4. You must take reasonable steps to ensure the data we hold is accurate and up to date
5. 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.
6. 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.
7. 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 DPO for logging and processing.
8. 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 DPO for logging and processing.
9. 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 DPO for logging and processing.
10. 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 DPO
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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).
17. Special care must be taken when dealing with sensitive personal data and data relating to criminal offences. Conditions set out in Articles 9 and 10 of the GDPR must be followed in every case.

How must I do it?

1. By following the requirements of this policy.
2. By following the requirements in the Privacy Notice Policy, the Consent Policy, the Clear Desk Policy, the Information Security Policy and the Privacy Impact Assessment Policy

3. By ensuring that the means you use to gather personal data (such as online or physical forms) only ask for the information required 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. 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.
6. By ensuring that all requests for personal data or other information under FOI/EIR are immediately referred to the DPO for initial consideration and to co-ordinate responses as required. This also includes requests to amend someone's personal data.
7. 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.

8. Consult the DPO 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**.**
9. By completing training courses relevant to your role.
10. By consulting the Data Protection Officer and/or I.T. Services to establish whether the proposed process is appropriate.
11. By carrying out a Privacy Impact Assessment when any change to processing personal data occurs or when a new system or process is put in place.

The Six Data Protection Principles

[Chapter 2] of the Data Protection Act lists the data protection principles in the following terms:
1. The processing of personal data must be lawful, fair and transparent
2. The purpose for which personal data is collected must be specified, explicit and legitimate and must not be processed in a manner which is incompatible with that purpose
3. Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data must be kept for no longer than is necessary for that purpose for which it is processed.
6. Personal data must be processed in a manner that includes taking appropriate security measures about risks arising from processing that data.

Breach Statement

A personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted stored or otherwise processed. Data breaches 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 the person concerned. The Council, as well as those individuals affected is also at risk of financial and reputational harm. Fines of up to €20,000,000 may be imposed for serious data breaches. You must report any actual or potential data breaches or other concerns relating to information governance to the Data Protection Officer as soon as possible.