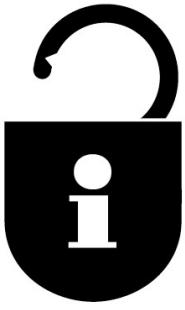
Bath & North East Somerset Council

Data Protection Act Policy



Risk & Assurance Service

Introduction

Bath & North East Somerset Council issue this policy in response to the Data Protection Act 1998 (DPA). This policy is also aligned to other legislation such as the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

The Council supports the aims of the eight principles of the DPA and is committed to processing personal data in a manner which is compatible with these Principles.

Scope

This Policy applies to all employees of Bath and North East Somerset Council including contract, agency and temporary staff, volunteers, and employees of partner organisations working for the Council.

In addition this Policy applies to all personal data processed by Elected Members as part of official Council duties. Members processing personal information in respect of their ward duties are not covered by this policy, and must make their own arrangements in regard to Notification.

This Policy does not apply to Primary, Secondary and Special Schools who are separate public bodies in their own right. They are statutorily obliged to make their own arrangements.

Electoral Services and the Registrar's Office are covered by this Policy; however they are required to provide separate Notification to the Information Commissioner.

Obligations

The Council is obliged to comply with the eight DPA principles.

The Council is also obliged to provide individuals with access to their own personal data. The DPA provides Data Subjects with a right of access to their own personal data (the right of Subject Access). Subject Access Requests must be responded to within 40 calendar days. Data Subjects are entitled to receive:

1. Confirmation of whether their personal data is being processed, and if this is the case;
2. A description of the personal data processed, of the purpose of the processing and of any Recipient or classes of Recipient.
3. A copy of the information, and information about the source if available.
4. Information about the logic of any automated decision that significantly affects them.

The Council is also obliged to consider requests to stop processing personal data, requests to prevent the processing of personal data for direct marketing

purposes or in relation to automated decision making, and requests to have inaccurate personal data corrected.

Principles

The Council undertakes to comply with the Data Protection principles when processing personal data. These require personal data to be:

1. Fairly and lawfully processed, and not processed unless one of the conditions in Schedule 2/3 of the Act is met;
2. Processed only for one or more specified and lawful purposes;
3. Adequate, relevant and not excessive;
4. Accurate and where necessary, kept up to date;
5. Not kept longer than necessary;
6. Processed in accordance with individuals' rights;
7. Kept secure;
8. Not transferred to non-EEA (European Economic Area) countries without adequate protection.

Charging

The Council will not make a charge for Subject Access Requests.

Complaints

If a Data Subject is unhappy with the response to their Subject Access request, or if they believe that the Council is processing their personal data in a manner which is incompatible with the Data Protection principles, they are entitled to request that an internal review be carried out. Requests for reviews should be made within 40 working days of the date of the original response. These reviews are conducted by the Divisional Director for Risk and Assurance Services, Mr Jeff Wring. Mr Wring is contactable at The Guildhall, 1 High St, Bath BA1 5AW. Email: jeff_wring@bathnes.gov.uk

If an applicant is unhappy with the outcome of the internal review, they have the right to appeal directly to the Information Commissioner for an Assessment. The Information Commissioner is contactable at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Monitor and Review

Should it be discovered that this Policy has not been complied with, or if an intentional breach of the Policy has taken place, the Risk and Assurance Service, in consulation with senior management, shall have full authority to take immediate steps as considered necessary, including disciplinary action.

The Policy will be subject to ongoing review in light of any changes in legislation or good practice, and will be formally reviewed on a regular basis, and at least annually.

Appendix to Data Protection Policy

Definitions

Data Controller	A person 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;
Data Subject	Any living individual who is the subject of personal data.
Personal data	Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. As well as including obviously personal data such as names and addresses (including e-mail addresses), the definition includes 'any expression of opinion about the individual and any indication of the intentions of the Data Controller … in respect of the individual'. The definition is therefore quite broad, and may cover information such as an individual's health, beliefs, personal hobbies, or business activities, for example.
Processing	Anything at all done to personal data, including but not limited to collection, use, disclosure, destruction and merely holding personal data.
Recipient	Anyone who receives personal data, except the Data Controller, Data Subject, or Data Processor.