

Access to Information Policy

Document Control

Document Ref:	WBC:SS:SCB:0812AtI	Date Created:	January 2014
Version:	V3, Replaces Access to Information Policy V2 approved May 2013	Date Modified:	
Revision due	January 2016		
Author:	Sue Broughton	Sign & Date:	27 th March 2014
Owning Service	Strategic Support		
Equality Impact Assessment: (EIA)	Date undertaken:	29 th January 2014	
	Issues (if any):	N/A	

Corporate Director (Resources Directorate)	Sign & Date:	Andy Day
Corporate Director (Communities Directorate)	Sign & Date:	
Corporate Director (Environment Directorate)	Sign & Date:	

Change History

Version	Date	Description	Change ID
1	2007	Access to Information Policy	
2	2013	Access to Information Policy	
3			



Contents

1. Purpose	3
2. Applicability	3
3. Policy	3
4. Implementation	4
5. Roles and Responsibilities	5
6. Failure to comply with the Access to Information Policy	6
7. Review	6
Glossary	6
Other Relevant Documentation	6
Annex 1: The Data Protection Principles	7

1. **Purpose**

- 1.1 The purpose of this policy is to ensure that West Berkshire Council complies with the requirements of the existing access to information legislation, including the Data Protection Act 1998, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and the Local Government Act 1972 Schedule 12A, and with any subsequent legislation.
- 1.2 The Access to Information Policy has been approved by Individual Executive Member Decision on [date].
- 1.3 This Policy applies to all requests for information made to West Berkshire Council, whether written or verbal, and to the security, confidentiality and administration of all personal information.

2. **Applicability**

- 2.1 This Policy applies to:
 - 2.1.1 All non-school based employees working for the Council, including those working from home or at non-Council locations.
 - 2.1.2 Other persons including Elected Members, Consultants, Agency staff and Contractors working for the Council, external organisations working with the Council, whilst engaged on Council business .
- 2.2 It is the responsibility of each employee and other person mentioned in Section 2.1.2 to familiarise themselves with and adhere to this Policy.
- 2.3 Adherence to this Policy is a condition of working for the council or using its assets.
- 2.4 This document is published separately as well as being incorporated into the the Council's Employee handbooks.
- 2.5 This Policy has had consultation with Heads of Service and Trade Unions and has been ratified by Individual Executive Member Decision.

3. **Policy**

- 3.1 It is the Policy of the Council to ensure that:
 - 3.1.1 All requests for information are acknowledged and dealt with promptly, and within the statutory timescales.
 - 3.1.2 Advice and assistance shall be offered to help any enquirer frame their request.
 - 3.1.3 Requests will be assessed to ensure that where applicable; the confidentiality of personal or commercially sensitive information is not breached; disclosure is in the public interest; and provision of the information would not be prejudicial to the provision of essential Council services.

- 3.1.4 Information shall only be withheld where a legitimate exemption applies, and in such a case, (where appropriate) the application of the exemption will be explained to the enquirer.
 - 3.1.5 Any enquirer shall be kept informed of the progress of their request, and of any delays to which it may be subject.
 - 3.1.6 Assistance shall be offered to any enquirer to help them understand the information they receive.
 - 3.1.7 All enquirers shall be advised of their rights to question the information received and request a review (where appropriate) of what has not been provided.
 - 3.1.8 All enquirers shall be advised of their right to take any complaint to an internal review process (where appropriate) or to the Information Commissioner, if they are dissatisfied with the service received or the information provided.
 - 3.1.9 Information which can be made publicly available shall be published under the provisions of the Publication Scheme to the West Berkshire Council website, or, where provided in response to a request, shall be published to the Council's Disclosure Log.
 - 3.1.10 All requests shall be monitored and performance indicators made available to demonstrate compliance with the legislation.
 - 3.1.11 All staff shall be provided with training, guidance and procedures to enable them to manage requests for information.
 - 3.1.12 Guidance will be provided for Members to enable them to identify, and respond to, or pass on to the public authority, requests made by their constituents.
- 3.2 Personal information, sensitive personal information and confidential information shall be stored, updated, transferred and protected as required by law, and as required for personal privacy, commercial sensitivity, and corporate security.
- 3.3 An officer or officers shall be appointed with specific responsibility for the administration of all requests for information made under the legislation cited in 1.1 (above).
- 3.4 The management of the access to information and Data Protection regimes shall be regularly audited to ensure compliance with statutory requirements and that relevant national codes of practice are followed.
4. **Implementation**
- 4.1 This Policy will be supported and implemented by the development and publication of Standards (requirements), Procedures (how to) and Guidance (advice) where required.

5. Roles and Responsibilities

- 5.1 The overall responsibility for access to information and Data Protection within the Council rests with the Chief Executive.
- 5.2 The responsibility for day-to-day management of access to information throughout West Berkshire Council rests with the Head of Strategic Support, who is also responsible for maintaining this Policy, for reviewing related procedures and for providing advice and guidance on their implementation.
- 5.3 All managers are directly responsible for implementing this Policy and any sub policies and procedures within their service areas, and for the adherence of their staff and others (2.1.2).
- 5.4 All personnel detailed at 2.1.1 and 2.1.2 have an individual responsibility to adhere to this Policy and any relevant Standards and/or Procedures.
- 5.5 All requests for personal data and Freedom of Information/Environmental Information requests will be logged and acknowledged centrally by the Information Management Officer or the Information Support Officer in Strategic Support.
- 5.6 All requests will be processed by a senior officer or officers in the relevant service, with advice and assistance from the Scrutiny & Partnerships Manager or the Information Management Officer in Strategic Support.
- 5.7 The requests procedure will be set out in the Data Protection procedure and the Freedom of Information procedure documents.
- 5.8 Training in the access to information legislation shall be provided for all officers, and regularly updated, with at least annual refreshers for Data Protection training. Responsibility for arranging and providing training rests with the Information Management Officer or the Information Support Officer in Strategic Support, in conjunction with the Training Team in Human Resources. Line managers are responsible for ensuring new starters undertake mandatory Data Protection training (induction and e-learning). Training will also be provided regularly by Strategic Support for Members
- 5.9 All officers processing personal data are required to comply with the Data Protection Principles (eight enforceable principles of good practice), as set out in the Act (relevant extract is in Annex 1 of this Policy). These provide that personal data must be:
- (a) Processed fairly and lawfully
 - (b) Processed for limited purposes and in an appropriate way
 - (c) Adequate, relevant and not excessive for the purpose
 - (d) Accurate
 - (e) Not kept for longer than necessary for the purpose
 - (f) Processed in line with data subjects' rights
 - (g) Secure
 - (h) Not transferred to people of organisations situated in countries without adequate protection

5.10 A Data Protection Subject Access Group will be convened to meet on a regular basis and consider performance monitoring, processes for handling requests, complaints about Data Protection issues, and training needs and competency issues. It will report to Corporate Board via the Strategic Support Senior Management Team.

6. **Failure to comply with the Access to Information Policy**

6.1 This document provides staff and others with essential information regarding access to information and sets out conditions to be followed. It is the responsibility of all to whom this Policy document applies to adhere to these conditions. Failure to do so may result in:

- withdrawal of access to relevant services
- informal disciplinary processes
- formal disciplinary action (in accordance with the Disciplinary Procedure)

6.2 Additionally if, after internal investigation, a criminal offence is suspected (for example under the Data Protection Act 1998), the Council may contact the police or other appropriate enforcement authority to investigate whether a criminal offence has been committed.

7. **Review**

7.1 This policy will be reviewed to respond to any changes and at least every 2 years.

7.2 The Service responsible for reviewing and maintaining this Policy is Strategic Support.

Glossary

Data Protection Act 1998 – An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding use or disclosure of such information.

Freedom of Information Act 2000 – An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records act 1958; and for connected purposes.

Other Relevant Documentation

Freedom of Information Act and Environmental Information Regulations Requests Procedures (in revision)

Data Protection Act Requests Procedures (in revision)

Security Policy

Standard - Protective Marking

Secure (Encrypted) Email Guidance

Annex 1: The Data Protection Principles

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.