Appendix 7(c)

WEST BERKSHIRE DISTRICT COUNCIL

Policy statement on Data Protection 2004

West Berkshire District Council supports the objectives of the Data Protection Act 1998 and other legislation relating to Data Processing, including the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and the Freedom of Information Act 2000. This Policy aims to assist staff with meeting their statutory and other obligations which covers the issue of Data Protection. This is an updated version of the original policy adopted by the Executive in March 2002.

This Policy will be held by the Data Protection Officer and a copy kept in Legal Services.

It will be updated and reviewed every two years.

What is data protection?

Data Protection is concerned with establishing a balance between freedom to process information on the one hand and the individual's right to privacy on the other. The Data Protection Act 1998 (DPA 1998) applies to both manual and computerised records and gives considerably enhanced rights to data subjects than previous legislation in this area.

The key points are the right of an individual to see the information held about them and the right to have that information corrected if appropriate.

Data Protection legislation applies when 'personal data' is 'processed '

'Personal data' is information which relates to a living individual and from which that individual can be identified.

'Processing' includes obtaining, recording, or holding data – this includes information contained in manual files, e-mails, telephones, faxes etc. (The legislation does not, however, apply to verbal communications.)

All organisations and individuals who 'process' 'personal data' are required to be registered with the Information Commissioner. Anyone who processes personal data is a data controller and must observe the eight Data Protection principles which govern the manner in which data is collected, held and processed.

These 8 Data Protection principles are detailed further on Page 3.

A glossary of terms is attached to this Policy at Appendix 1.

West Berkshire District Council (WBDC)
WBDC is registered with the Information Commission as a 'data controller ' under the DPA 1998.

Some information, for example, the electoral register is publicly available by law and its publication is therefore not restricted by the DPA1998.

WBDC, as a Local Authority, holds vast amounts of personal information – about residents, local businesses, voluntary organisations etc. As a data controller, the way this information is regulated and stored is covered by the Data Protection Act 1998. WBDC works with a number of external bodies to assist in the provision of services. This policy will apply to external partners engaged in Council work.

The Council is committed to ensuring that all information held is necessary, used fairly and responsibly and in compliance with the eight Data Protection Principles

WBDC keeps personal information to assist in the provision of services to the public. These services include but are not limited to:-

Community Care
Housing
Older Peoples Services
Quality Services
Children & Families
Education Services
Culture & Youth
Information & Communication
Public Protection
Planning & Transport
Highways & Engineering
Countryside & Environment
Information & Communication
Legal & Electoral Services
Policy and Performance
Scrutiny
Procurement
Property
Revenues & Benefits
Service Access
ICT & Business Support
Organisational Development & Human Resources

The Head of Service will have overall responsibility within that Service for data protection and will act as 'data protection service controller' for that Service.

Each Service Area, in addition to a data controller must have a Data Protection Service Representative. The role of the Service Representative is

to attend meetings of the Data Protection Working Group and to feed into and implement actions of the Working Group to their particular Service. The Service Representative shall assist the Data Protection Service Controller to co-ordinate and maintain the implementation of the Data Protection policy in their own Service. The Service Representative will have assistance in these tasks from the Data Protection Controller and from colleagues within their Service.

The 8 Data Protection Principles and their practical effect

WBDC seeks to ensure that the processing of personal data complies with the 8 Data Protection principles which require personal data to be :-

1. Processed fairly and lawfully

- *Information will only be held where it is justified to do so and processing may be carried out where one of the following conditions has been met, namely where:-*
- *The individual has given their consent to the processing*
- *The processing is necessary for the performance of a contract*
- *The processing is required as part of a legal obligation*
- *The processing is necessary to protect the vital interests of an individual*
- *The processing is necessary in order to pursue legitimate interests*

Local Authorities have specific legal authority to use or disclose information under duties or powers given to them under statute. For example, information obtained by the Council Tax department may be used or disclosed for council tax purposes. Providing that data is being processed in accordance with Council Tax use, such data will be being processed lawfully.

2. Processed only for the specified lawful purposes and not processed in any way incompatible with those purposes

- *The Council has many different statutory functions. Some services may hold details of residents for one function whilst others hold the information for another. This does not necessarily mean that the information collected for one purpose can be used for another.*

- *Data held for more than one function by more than one service by the Council will be collected and processed independently. It should not be assumed that information can be passed to another department for a different purpose automatically unless there is clear justification to do so. (For example, for the prevention or detection of a crime)*

- *Neither should it be assumed that because information is held by the Council for a specific purpose that it should automatically be shared with another Local Authority or another voluntary organisation.*

- *All requests for information from other public bodies, including the police, are to be in writing and on headed paper.*

- *When receiving requests for information, clarification must be obtained as to who the requesting party is, the reason why information is requested and if there is authority to give the information.*

3. **Adequate, relevant and not excessive in relation to the purpose(s) for which personal data is processed**

- *WBDC will only hold the minimum personal information necessary to enable it to perform its functions.*

4. **Accurate and kept up –to – date**

- *All efforts will be made to ensure that information is periodically assessed for accuracy and is kept up to date.*

5. **Processed no longer than is necessary for the purpose(s)**

- *Information **must** be destroyed once it is no longer required*

6. **Processed in accordance with the rights of the data subject**

- *WBDC recognises the rights given to people under the DPA 1998 including the right to access information, the right to have inaccurate information corrected or erased and the right to entitlement to compensation should any damage be suffered as a result of any breach of the DPA 1998 principles*

7. **Protected by appropriate and organisational measures**

- *WBDC has systems in place to keep information secure. A separate section entitled 'Storage and Security' is on page 8 of this Policy.*

8. **Not transferred to any country outside the EU unless that country has an 'adequate level of protection' in respect of data protection**

- *WBDC operates its own website which is obviously accessible by countries outside the EU and which involves the transferring of data on an international basis. The website provides structured information about WBDC, its staff and the services which WBDC provides. Where personal data regarding individuals or companies is published on the website, consent from the data subject must be obtained prior to any personal details being published.*

- *There may also be times when WBDC will receive a specific request to transfer specific data to another country. If this situation arises, the necessary enquiries will be made as to whether the transferee country has adequate data protection. If not, information will not be transferred. Data can, however, be transferred to any country, even if outside the EU, if the data subject has given their consent to disclose.*

Sensitive Personal Data

There are additional requirements placed upon the data controller where the holding of 'sensitive personal data' is concerned.

The definition of 'sensitive personal data' is data in respect of: -

A. racial or ethnic origin
B. political opinion
C. religious belief
D. union membership

E. physical/mental health
F. sexual life
G. commission of offences
H. proceedings for offences and sentences of Court

If disclosing sensitive personal data (even if required to do so by law) consent of the data subject should be obtained unless a specific exemption applies. If an exemption is considered to apply, it may be prudent to inform the data subject of the information given to the third party and the reason why such information has been disclosed. This decision should be made at senior level and the reasons for disclosure well documented. Each service must have recorded the level of seniority at which data protection decisions should be made. In the absence of such a record the Head of Service will be responsible for such decisions.

Additionally, if sensitive personal data is held, security measures for holding such data will need to be considerably higher than that for other service areas holding less sensitive data. In all cases where sensitive personal data is held, the Service must have a record of the justification and reasons for holding such data together with the procedures for ensuring confidentiality.

Subject Access Requests – What the Data Protection Service Controller (i.e. the Head of Service) has to do

Under the Data Protection Act 1998, data subjects have the right to know what information is held about them. This is known as a Subject Access Request.

The procedure for dealing with Subject Access requests is contained in the WBDC publication – 'Personal Information : Your Right to know' which is also the application form on which to make a Subject Access Request.
If a data subject wishes to make a subject access request, they should be asked to complete the application form ('Personal Information: Your Right To Know)
Requests for information should be sent at first instance to the Data Protection Officer:-

Sue Curtis Davidson
Head of Information and Communication Services
Market Street Offices
Newbury
(t) 01635 519974

The Data Protection Officer will then pass to the Data Protection Service Controller in the relevant Service Area to action the request. If the Data Protection Service Controller is unable to deal with the request or requires clarification, they should revert to the Data Protection Officer.

A maximum fee of £10 per request will be charged, although in respect of access to Social Services files, the charge of £10 will be at the discretion of the Data Protection Service Controller within Community Care and Children and Families Services.

Employees of WBDC will not be charged for access to their records.

The Data Protection Service Controller will respond within the statutory time limit of 40 days by making the information available to the data subject.

If the Data Protection Service Controller considers that an exemption applies and does not consider that disclosure is appropriate, the data subject must also be informed of this within 40 days of making the request.

If an exemption is considered to apply, the decision not to disclose information should be made at senior level and the reasons for non-disclosure documented.

In considering whether to disclose information, the Data Protection Service Controller must take care not to reveal the identity of another third party individual. Any information supplied by a third party should not usually be revealed without first seeking permission from the source.

In addition, the data subject also has a right to have inaccurate information corrected, blocked or erased. If a request to amend information is received from a data subject, the Data Protection Service Controller must respond within 21 days to confirm what action has been taken. Any decision would be taken by a senior member of staff and the reasons documented.

The data subject also has a right to know the process and information involved in any automated decisions regarding them. If the data subject objects to the decision made by automated decision, a further decision should be made by other means if possible. The data subject has 21 days in which to request a further decision be made by non-automated decisions and the data controller has 21 days to action.

Requests made on behalf of children

A request for information may be made by a parent, guardian or agent on behalf of another individual.

Requests made on behalf of others will be dealt with as above, however care should be taken to verify the identity of those making the request if there is any doubt.

Nothing is to be disclosed to a third party which would not be in any child's best interests to do so. This includes where information is requested on the child's behalf by any parent or Guardian. The decision as to what not to disclose should be made by the Data Protection Service Controller and the reasons for any non-disclosure documented.

Requests made by children

Requests by children can be made to a number of services, including Childrens' Services, Education and Culture and Youth Services.

Any child may be allowed to see their own records unless it is obvious that they do not understand what they are asking for.

Again, the Data Protection Service Controller should consider that nothing be disclosed to a child which would be likely to cause serious harm to their physical or mental health. The decision as to what not to disclose should be made by the Data Protection Service Controller and the reasons for any non-disclosure documented.

There will be no fee charged for requests made by children under the age of 18. In respect of children who are or have been in the care of the Authority there will be no charge where the child or young person is under the age of 25. Information for Looked After Children on how to access their records is contained in the Young People Information Pack, published by Social Services.

In addition, the usual principles of subject access requests as outlined in this policy will apply.

Disclosure to a Third party

Any request for data where received by a third party should be in writing and the third party must be identified. Where the third party seeks to rely on a legal authority for disclosure they must quote the relevant authority.

Unless an exemption applies (see below), personal data will not be disclosed, save where the data subject consents to such disclosure.

'Third party' includes members of a data subject's family, legal representatives of a data subject , a data subject's employer and any organisations acting on behalf of an individual such as the Citizen's Advice Bureau or a Housing Association.

Requests for access from a third party should be accompanied by either an Authority to Disclose from the data subject or in the absence of this, necessary enquiries should be undertaken by the Data Protection Service Controller to ascertain if consent is given. If there is any doubt, written confirmation direct from the Data Subject should be sought.

The 40 day time limit also applies to requests for data from a third party, including the requirement to inform why a decision for not disclosing is made and the reasons for doing so. Again, this decision should be taken by a senior member of staff and the reasons for not disclosing documented and made clear to the third party.

Nothing should be disclosed which would be likely to cause serious harm to a child's or vulnerable adult's physical or mental health. In all requests for access, the interests of the subject, particularly in the case of a child or vulnerable adult must be paramount and the duty of the Council to protect children and vulnerable adults from potential harm of primary importance.

Exemptions

The rights of data subjects are subject to certain statutory exemptions. The Council will disclose personal information, without the data subject's consent in accordance with the DPA 1998.

This includes but is not limited to: -

- On production of a court order for disclosure
- Where the purpose of disclosure is to enable the Authority to assess or collect any tax or duty or any imposition of a similar nature
- Where the purpose of disclosure would be to prevent or detect a crime, apprehend or prosecute offenders
- By order of the Secretary of State
- Where we are obliged by any law to disclose information
- Where information is required for research purposes providing such data is general and does not cause damage or distress to the data subject
- Where disclosure would be to safeguard national security
- To WBDC councillors, **where disclosure is necessary to enable them to fulfill their statutory duties as Councillor**, for example where the Councillor is a member of a specific committee or when acting on behalf of a Constituent. NB: Councillors are not automatically entitled to information, particularly sensitive information – see below at Page 10 'Disclosure to Members'

Storage and Security

Personal data will only be kept for as long as the service provided to the data subject is in existence or is as required by law. If there is no legal requirement to keep the records, they will be destroyed as soon as is practicable. Where there is no legal requirement, information is not normally kept for more than 12 years.

Each service area also needs to consider carefully what records it needs and, in particular, whether any legal proceedings may arise which the information could assist with.

There are some records which must be kept for longer, including adoption records and records in respect of children in care.

There is a corporate Record Retention policy, which covers all service areas.

Maintenance and security of information is the responsibility of the department of the authority providing the service. Each service must identify all computer and manual systems within their Service which contain information about individuals and ensure compliance with this Policy statement. In the case of school pupil records, the responsibility is the schools' and the individual teachers'.

Computerised files are protected by password within the offices at WBDC and manual files holding data are kept in controlled access secure areas.

No private use shall be made of any personal data or information belonging to WBDC by any employee, nor shall any computer belonging to an employee be used for Council work without the written permission of the relevant line manager. In the event that employees take home manual or computerised files containing data, it is the employee's responsibility to ensure that such data is made secure.

The use of unlicensed software and the unauthorised use of any computer or system is strictly prohibited, nor shall any computer be knowingly exposed to the risk of any virus type infection.

All documents containing personal data are to be disposed of as confidential waste.

Any computer screen which can be viewed by the public, for example in reception areas or libraries which holds personal data shall be re-positioned to minimise the opportunity for the public to inadvertently view personal data. Any papers which hold personal data and which is potentially accessible to the public, for example on front line services should be kept confidentially and out of sight to the public.

Computers should be wiped of any personal data before being disposed of or sold.

Elected Members

Councillors must ensure that Data Protection legislation and policy are complied with whatever role they may exercise. If the Member is in any doubt, they should contact the Data Protection Service Controller and/or the Data Protection Officer for clarification.

Where Councillors sit as the Council's representative on an outside body, the Councillor's duties will vary depending on the nature of the role taken but in the case of a Trustee or Director, they will owe a duty to the organisation on which they sit. In addition, since May 2002 Councillors have been subject to the Code of Member Conduct, which includes duties in relation to information acquired or received in confidence.

Where the Councillor is required to act as WBDC's representative on other public sector bodies, joint boards, working parties etc, their status will be the same as if they were an employee of the Council. However, councillors must not use their position as a representative to secure services for individual constituents. Conversely, councillors must not pass on any personal information acquired as a Member to any outside body.

When Councillors are required to act as WBDC's appointed representative on Local Government National Bodies, the Councillor's responsibility will be towards the body, which made the appointment and not WBDC in the first instance.

If members of a specific political party, Councillors will also be subject to any Data Protection conditions established by the organisation concerned.

Councillors will be data controllers whenever they process personal data for their own purposes.

This may include but is not limited to the following: -

- Constituency case work
  - where the Councillor is not carrying out their official duties but is acting in a personal capacity
- Canvassing political support
- Processing of personal duties held in connection with duties as a representative of a National Body
- Processing of personal data held and processed as part of the Councillor's own business or profession

If a Councillor seeks clarification over whether they are processing data as a separate data controller from WBDC, councillors can obtain a copy of 'Data Protection: A Councillor's Guide' which is held by the Data Protection Officer. Information for Councillors is also available from the Information Commissioner's Website at www.informationcommissioner.gov.uk.

If the Councillor is processing data for their own purposes they must register with the Information Commission as a data controller as well as ensure compliance with the principles of the DPA 1998.

Councillors are also data subjects and as such, have the same entitlements as any other individual under the DPA 1998 regarding personal information held about them.

(i) Disclosure to Members

Generally, the Council does not have to obtain the consent of the data subject for disclosure to the Member provided the Member represents the ward in which the data subject lives (in which case it is presumed that the Member acts on behalf of the data subject)

However, where disclosure is made of sensitive personal data (as defined on Page 4) the consent of the data subject is required. Care must also be taken not to disclose anything which will be at variance with the needs of a child or vulnerable adult whose interests must be paramount. In addition, it is vital that information disclosed to Members is accurate and up to date.

Some court proceedings, for example ongoing child care proceedings, are confidential and must remain so. Similarly, Child Protection investigations are confidential. Any information forming part of such court proceedings or investigation is highly unlikely to be able to be disclosed to a Member, even where the Member represents the ward in which the data subject lives.

When providing information to any Councillor, the Data Protection Service Controller for the Service should make a note of the request and make clear

to the Councillor that the information is provided only for the limited purpose of assisting the data subject.

Where the information is requested by Elected Members for political purposes, consent of the individual data subject should be obtained except if the Council is required to make certain data public, (for example lists of certain types of licence holders) or if information disclosed does not identify living individuals.

Generally, members are not treated as separate data controllers but are regarded as being within WBDC for the purposes of data protection.

Where the councillor receives personal data from WBDC about individuals in order to enable him/her to carry out their statutory duties as a member of the Council, the Councillor's use of the data is subject to this policy as though the Councillor were an employee of WBDC. Personal data will be treated as **confidential** and the requirements in respect of disclosure to third parties will apply.

(ii) Disclosure by Members
Members, in accordance with this policy, may only disclose information to third parties where certain circumstances arise. This includes but is not limited to: -

- On production of a court order for disclosure
- Where the purpose of disclosure is to enable the Authority to assess or collect any tax or duty or any imposition of a similar nature
- Where the purpose of disclosure would be to prevent or detect a crime, apprehend or prosecute offenders
- By order of the Secretary of State
- Where we are obliged by any law to disclose information
- Where information is required for research purposes providing such data is general and does not cause damage or distress to the data subject
- Where disclosure would be to safeguard national security

This does not mean that if one of the above exemptions applies that information will be disclosed automatically. Members must consider all the circumstances of the particular request before applying any exemption. In particular, the Member must consider whether disclosing any information would harm the interests or safety of any child or vulnerable individual.

Additionally, Members must ensure that where disclosing any information, that such information is accurate and up to date. Even when information is requested by other service users residing in the Members' area, the Member is prevented from disclosing information to them unless consent of the data subject has been given or unless a clear exemption applies.

Compliance with the DPA 1998

The Council recognises the need to make the contents of this Policy Statement known and ensure compliance by every employee.

It is the responsibility of Managers and Head Teachers to ensure compliance with this Policy Statement.

A copy of the list of the Data Protection Representatives for each Service Area will be held in Information and Communication and in Legal.

Front line staff, such as reception staff will be trained and made aware of this Policy and of WBDC publications available.

All Councillors shall be provided with a copy of the Guidance on the Implications of the DPA 1998 for Councillors entitled ' D.P. – A Councillor's Guide'. Members will also receive training in Data Protection policy where necessary.

The Council also recognises the need to make their Policy known and accessible to the public. The request for data subject access should be made on the WBDC publication 'Personal Data: Your Right to know' which is available to the public at Council receptions and libraries. This form also contains some information for the public as to the Council's Policy on Data Protection.

An internal review of Notification requirements will be undertaken by the Data Protection Officer from time to time and the Information Commission informed of any changes required in notification.

Training updates for Data Protection Service Controllers and Service Representatives will also be provided as and when required.

Failure to comply with Legislation and Policy

WBDC expects all employees to comply fully with this Policy, the Data Protection principles and the Council's Employee Handbook. Disciplinary action may be taken against any Council employee who knowingly breaches any instructions contained in, or following from this Data Protection Policy.

Individual employees are affected in the same way as the Council as a whole. Anyone contravening the Act could be held personally liable and face court proceedings for certain offences which may result in a fine.

If any of the principles of the Data Protection Act 1998 are breached, the data subject may be entitled to compensation and/or a decision may be made by the Information Commissioner or the Information Tribunal for their records to be amended.

(Similarly, the Information Commissioner or Information Tribunal may decide to uphold a decision of the Council following a decision not to disclose or amend information held.)

The Information Commission has power to investigate any aspect of a Data Controller's data processing of personal data and if need be, has powers to cause the processing to cease

The Information Commission also has powers of entry and inspection into the premises of a data controller and in some circumstances has power to fine data controllers for an unlimited amount.

Other rights of the individual

This policy shall not affect or in any way compromise an individual's rights under the Human Rights Act 1998.
The individual also has rights under the Freedom of Information Act 2000. At present an individual's right to privacy outweighs another individual's right to information under the Freedom of Information Act (i.e if personal data is contained in a document that document cannot usually be released to a third party)
The Council is developing a Freedom of Information policy for full implementation of the Act in January 2005 and this Data Protection Policy should be read in conjunction with the Freedom of Information Policy.

Caldicott

This policy should be read alongside the Caldicott review. The Caldicott principles and processes, issued by the Department of Health, provide a framework of quality standards for the management of confidential information within Health and Social Care services.

The Caldicott requirements provide a set of good practice guidelines to assist in the implementation of the Data Protection Act and underpin appropriate information sharing. However, it is the Data Protection Act that is the key legislation covering all aspects of information processing, and therefore takes precedence.

APPENDIX 1 – DEFINITIONS

The following terms appear throughout this Policy and are defined here in order to assist understanding of the key requirements of Data Protection Data

Information which –

a. Is processed by means of equipment operating automatically in response to instructions given for that purpose
b. Is recorded with the intention that it should be processed by means of such equipment
c. Is recorded as part of a relevant 'filing system', or with the intention that it should form part of a relevant filing system
d. Forms part of an 'accessible' record
e. Any recorded information held by a public authority including information held by a public authority on behalf of others

Data Subject
The data subject is an individual who is the subject of personal data.

Subject Access
This is the right which each individual has to access personal data held about him/her by a data controller.

Personal Data
Personal information which relates to a living individual who can be identified from that information and other information in the possession of the data controller. This includes expressions of opinion regarding the individual.

Processing
Means obtaining, recording or holding the information, or carrying out any operations on the information. This includes organising, adapting, altering, retrieving, consultation, use and disclosure of the information. It also includes erasing or destruction of the data and making the data available including by way of transmission.

Data Protection Officer (t) 01635 519974

A person with overall control of data protection issues within WBDC.
The WBDC's Data Protection Officer is :-
Sue Curtis Davidson
Head of Libraries, Information and Technology, Market Street Offices

Data Controller
A person who determines the purposes for which and the manner in which any personal data are, or are to be processed. WBDC is a data controller.

Data Protection Service Controller
In this policy, this means the Head of Service from each Service Area. The DP Service Controller has overall responsibility within their Service Area for data protection issues.

Data Protection Service Representative
Will represent their service at meetings of the Data Protection Working Group and have responsibility for co-ordinating and implementing their service specific data protection policy.