



Data Protection Policy

Prepared By: Malkiat Thiarai
Head of Corporate
Information Management
Date of Publication: 04 January 2012
Version: 4.0
Classification: Not Protectively Marked

Table of Contents

1. Version Control	3
2. Points of contact for this Policy	3
3. Purpose of Data Protection Policy	4
4. Overview of the Data Protection Act 1998	4
5. Confidentiality and Security.....	5
6. Ownership of Data	6
7. Obtaining, Recording, Using and Disclosing	7
8. Data Subjects Rights	8
9. Use of Children’s Data.....	9
10. Use of Risk Markers.....	10
11. Shielded Records.....	11
12. Training.....	11
13. Security.....	12
14. Framework Code of Practice on Information Sharing	12
15. Data Protection Guidance	12
16. Related Guidance.....	13
17. Compliance - Related Legislation.....	13
18. Definitions	14

1. Version Control

Version	Date	Notes
Draft	08 th March 2006	Awaiting
1.0	13 th March 2006	Updated following review
1.1	17 th March 2006	Updated
1.2	31 st March 2006	Draft sent out to DP Contacts for comments
1.3	8 th May 2006	Updated
1.4	21 st June 2006	Updated
1.5	7 th July 2006	Updated and complete
1.6	8 th August 2006	Updated with additional comments
1.7 DRAFT	3 rd December 2007	Annual Review, no changes
2.0	11 th December 2007	Approved by BTAG
2.1	13 th December 2007	Changed Information Classification & Handling Policy to IS Classification Standard and IS Labelling and Handling Standard (which replaced the policy)
2.2	1 st December 2008	Inclusion of Information Sharing Code of Practice and Privacy Notice. Following discussions at the FOIWG meeting 25 th November 2008.
2.3	28 th September 2009	Updated following workshop 10 th September on the use of Children's Data including Guidance Note on the use of children's data. Sent to DP Contacts for comment
2.4	22 nd October 2009	Updated with additional comments sent to DP contacts to circulate to relevant officers
2.5	1 st December 2009	Updated and Complete for approval by BTAG
2.6	15 th September 2010	Initial changes following 9 th September workshop on use of Risk Markers / Shielded Records
3.0	8 th December 2010	Approved by BTAG
3.1	20 th December 2011	Updated following annual review and comments
4.0	4 th January 2012	Approved by BTCG

2. Points of contact for this Policy

Document Author

Name	Malkiat Thiarai
Title	Head of Corporate Information Management
Telephone	0121 303 1909
Email	Malkiat.thiarai@birmingham.gov.uk

3. Purpose of Data Protection Policy

3.1 Scope

It is the Council's obligation to ensure compliance with the Data Protection Act 1998. The Information Commissioner, who oversees compliance and promotes good practice, requires all data controllers who process personal data to be responsible for their processing activities and comply with the eight data protection principles of 'good information handling'.

These are:

1. Personal data shall be processed fairly & lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and, where necessary kept up to date.
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of data subjects
7. Security principle - Protection against unauthorised /unlawful processing
8. Transfers outside of the EEA - Requires adequate levels of protection

Data Protection law and policy aims to ensure that individual's rights and freedoms are protected. Using personal data to abuse discriminate or deny access to services is unlawful. The City Council is committed to ensuring that personal data that it holds is used fairly and lawfully and in a non-discriminatory manner.

This policy applies to all personal data held by Birmingham City Council. It encompasses manual/paper records and personal data electronically processed including information gathered on CCTV systems, of whatever type and at whatever location, used by or on behalf of the City Council.

Companies and organisations will hold information of a personal nature about people. If this information is collected or entered wrongly, is out of date or is mixed up with someone else's personal data, it could cause complications as a result. A number of problems could occur as a result of this, such as being refused credit, unfairly refused a job or even arrested in error because of a mistake being made to the personal information held.

4. Overview of the Data Protection Act 1998

4.1 Overview

The Data Protection Act 1998 gives individuals the right to see information about them held by companies and organisations. In certain circumstances they may have the information corrected or erased, or they may even be able to prevent the processing of their personal data. If a Data Controller causes an individual damage or distress as a result of non-compliance, they could claim compensation. The Council is classed as a Data Controller and could be prosecuted for any serious offences that may be committed.

The Data Protection Act 1998 is not optional. It is mandatory and there can be harsh penalties imposed for non-compliance with the Act. In a Crown Court fines can be unlimited and all organisations processing personal data can be affected.

4.2 How this impacts on employees of the Council

The obligations outlined in this policy apply to all those who have access to personal data held by Birmingham City Council, whether employees, agency staff, elected members (or other public representatives), trustees, employees of associated organisations or volunteers. It includes those who work at home or from home or have remote or flexible patterns of working.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or is deliberately acting outside of their recognised responsibilities may be subject to the Council's disciplinary procedures, including dismissal where appropriate, and possible legal action liable to prosecution. All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the job/position being undertaken.

As well as the Council, individual employees can also be prosecuted for unlawful action under the Act. Upon summary conviction (in a Magistrate's Court), fines of up to £5000 could result if employees process information about other people without their consent or proper authorisation from the Council. Upon conviction or indictment (Crown Court), the fine can be unlimited. Employees could be committing an offence by sharing information with other employees who do not need to be told that information in order to carry out their legitimate Council duties.

4.3 New Powers given to Information Commissioners Office

The Criminal Justice and Immigration Act has created tough new powers for the Information Commissioners Office. This new legislation gives the ICO the power to impose substantial fines on organisations that deliberately or recklessly commit serious breaches of the Data Protection Act 1998.

The ICO's new power to issue monetary penalties came into force on 6 April 2010, allowing the ICO to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act 1998.

The ICO has produced statutory guidance about how it proposes to exercise this new power, which has been approved by the Secretary of State for Justice. The first fines were issued by the ICO in November 2010.

5. Confidentiality and Security

5.1 Confidentiality and Security

Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles as defined in the Data Protection Act 1998. Confidential information can be the most valuable asset of a business and employees will automatically have duties to their employers to ensure that confidential information is not knowingly or recklessly misused. For more information see the City Councils':

- Information Security Classification Standard
- Information Security Labelling and Handling Standard
- Access Control Standard
- Disposal of Information Processing Equipment Standard
- Email Code of Practice and Lawful Business Regs Notice

- Email Use Policy
- Flexible and Remote Access Standard
- Information Security Labelling and Handling Code of Practice
- Information Security Policy
- Password Control Standard

These and other policies relating to Information Security and IT security are available on Policies Standards Procedures and Guidelines database (PSPG) on Lotus Notes.

- Manual files (paper records) - access must be restricted solely to relevant staff and stored in secure locations (e.g. lockable cabinets), to prevent unauthorised access.
- Computer systems will be configured and computer files created with adequate security levels to preserve confidentiality. Those who use the City Council's computer equipment will have access only to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work. A Statement of Access document should be completed to identify who is authorised, what they are authorised to see.
- Data users must comply with the Council's Security measures.
- Personal data will be disclosed only to the data subject and other organisations and persons who are pre-defined as notified recipients within the City Council's Notification Register Entry held with the Information Commissioners Office. At certain times it may be required that personal data is disclosed under one of the exemptions within the Data Protection Act 1998. If there is a requirement for this an audit trail will need to be kept to provide accurate records of any disclosures of personal data.
- Preventing abuse and discrimination. The Council processes **sensitive personal data** (as defined in the Act) on employees and services users. The Council will have regard to its various diversity policies to ensure that if instances of abuse or discrimination occur, appropriate action is taken

Sensitive Personal data consists of the following information as to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed

6. Ownership of Data

6.1 Ownership of Data

Each City Council directorate is responsible for the personal data that it holds. This responsibility also extends to personal data that is processed by a third party on behalf of the City Council. The directorate will hold a record of all processing activities containing personal data, whether paper based or electronic. Where required, the directorate will provide the necessary information to the Corporate

Information Governance Team in order to facilitate the notification of the data with the Information Commissioner.

Internal notification is the process by which the Council keeps a check of processing activities in terms of the personal data it holds. This process is currently undertaken by the Corporate Information Governance Team who have responsibility of ensuring the Council's Register Entry with the Information Commissioner is kept accurate and up to date. Failure to do this is a criminal offence

Each directorate should have in place a contact officer who oversees data protection within their own directorate. They are the first points of contact and also responsible for notification within their directorate. This process is helped by the use of a corporate notification database that lists all the current systems that are processing personal data.

As part of the annual assurance statement process managed by Birmingham Audit statements will include assurance on the use and handling of personal data.

Changes to the way that services are delivered will require consideration of the use of personal data and appropriate data protection considerations.

7. Obtaining, Recording, Using and Disclosing

7.1 Processing

Each of these activities comes within the definition of **processing**. Processing in relation to personal data, means carrying out any of the processing activities "on the data"

Any activity/operation performed on personal data - whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data.

This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. *(It is difficult to envisage any activity, which does not amount to processing)*

All processing of personal data will comply with the Data Protection Principles as defined in the Data Protection Act 1998. In the situation where a third party processes data, the third party will be required to act in a manner which ensures compliance with the Data Protection Act 1998 and have adequate safeguards in place to protect the personal data.

7.2 Recording and using the data

Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the data subject.

The City Council will endeavour to inform all individuals of why their personal data is being collected. In line with the first data protection principle all information will be collected fairly and lawfully and processed in line with the purpose for which it has been given. The City Council may need to hold and process information in order to carry out any statutory obligations, where this process takes place all personal data will be processed fairly and lawfully.

7.3 Obtaining

It is a requirement that any data collection forms used in order to collect personal data will contain a "**fair obtaining**" statement. The statement will need to be clearly visible and placed appropriately so the data subject (individual to whom the information relates) is fully aware of the intended uses of their personal data.

The information that would need to be supplied on a data collection form is as follows:

- The identity of the data controller or appointed representative
- The purpose or purposes for which the information is intended to be processed
- Any foreseen disclosures of the information to be obtained; and
- Any further information in order to make the processing fair.

It is also very important to remember that when collecting data via the telephone or face to face the above information should also be made clear to the data subject before any processing of their personal data takes place.

7.4 Privacy Notice

As part of the Data Sharing review carried out by Richard Thomas and Dr Mark Walport, published in July 2008, it was recommended that organisations took steps to increase transparency. Fair Processing Notices should be much more prominent in literature, both printed and on line, and written in plain English. It was also recommended that the term Fair Processing Notice should be changed to Privacy Notice, and that they should state what personal data they are holding, how they use it, who can access it, with whom they share it, and for how long they retain it. The Council has adopted this recommendation. The relevant guidance can be found in guidance note 6 The Fair Processing of Personal Data.

7.5 Disclosing

Personal data must not be disclosed, except to **authorised** users, other organisations and people who are pre-defined as a **notified recipient** or if required under one of the **exemptions** within the Data Protection Act 1998.

8. Data Subjects Rights

8.1 The Right of Subject Access (sections 7 to 9)

A written request received by a Data Controller (Birmingham City Council) from an individual wishing to access their rights under the provisions of the Data Protection Act 1998 is known as a Subject Access Request. Sections 7 to 9 of the Act gives an individual the rights to request access to any 'personal data' that they believe may be held about them. This can include requests from children under the age of 16 (or those acting on their behalf).

If it does hold the requested information, then it will provide a written copy of the information held about them and details of any disclosures which have been made. The information requested will be provided promptly and in any event within 40 calendar days of receipt of the subject access request. If the information cannot be disclosed within the time period specified, the data subject will be kept fully informed

of the process and given access to any personal data that may already have been gathered.

If the data subject believes that Birmingham City Council has not responded correctly and are not happy with the Council's response to their concerns they are able to complain to the Information Commissioner.

8.2 Prevention of processing causing damage or distress (DPA section 10)

If an individual believes that a data controller is processing personal data in a way that causes them substantial unwarranted damage or substantial unwarranted distress, they can send a notice (data subject notice) to the data controller requesting, within a reasonable time, the data controller to stop the processing.

8.3 Right to prevent processing for purposes of direct marketing (DPA section 11)

An individual is entitled to request (in writing) a data controller to cease, or not to begin, processing their personal data for the purpose of direct marketing. When a data controller receives a written notice they must comply as soon as practically possible.

An individual may apply to a Court for an order if the data controller fails to comply with a written notice.

8.4 Rights in relation to automated decision taking (DPA section 12)

An individual is entitled, by written notice, to require a data controller to ensure that no decision, which significantly affects that individual, is based solely on the processing, by automatic means, of personal data of which that individual is the data subject.

8.5 Right to compensation (DPA section 13)

An individual who suffers damage, or damage and distress, as the result of any contravention of the requirements of the Act by a data controller, is entitled to compensation where the data controller is unable to prove that they had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

8.6 Dealing with inaccuracy (DPA section 14)

A data subject may apply to the Court for an order requiring the data controller to rectify, block, erase or destroy such data relating to that data subject as are inaccurate together with any other personal data relating to the data subject which contain an expression of opinion which the Court finds is based on the inaccurate data.

9. Use of Children's Data

The Council uses children's data to deliver a wide range of services to children and young people. These range from leisure and cultural services to education and care services.

Data protection law (at European and domestic level) does not draw any explicit distinction between data subjects who are adults and those who are children. Rather, it works on the basis of whether the individual is able to give consent to the processing of their data, with the full understanding of the implications of providing such consent, especially in light of the data processed.

Therefore, in using children's data, consideration should be given to ensuring that data protection principles are appropriately applied. These will include obtaining consent for the use, processing and sharing of the information.

The Information Commissioners' guidance suggests that children from the age of 12 will have the capacity to give valid informed consent for the processing of their personal data. However, this need to be considered in the context of the services being provided and other legal obligations that the Council needs to follow. Guidance note 10 considers this issue in further detail.

10. Use of Risk Markers

As an employer, the City Council has a duty of care to their staff to protect them at work. Health and safety legislation such as the Health and Safety at Work Act 1974, Management of Health and Safety at Work Regulations 1999 and the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 provide the legislative framework to which employers must comply when considering how to protect staff at work. Further information in respect of Health and Safety obligations can be obtained from the Corporate or Directorate Health and Safety teams.

Risk Marker is defined as: a measure of risk that the customer represents to council staff or sub-contractors, via any face to face or verbal interaction. This risk could be one or many of a wide range of factors such as risk of inflicting physical harm, or verbal abuse, or risk when visiting a location.

The use of Risk Markers as a means of identifying and recording individuals who pose, or could possibly pose, a risk to the members of staff who come into contact with them, is in practice, a flagged piece of text attached to an individual's file. These markers should be used very carefully and should contain the reasons for identifying individuals as presenting a risk. They are likely to record information relating to:

- the nature of the apparent risk posed by interaction with an individual; or
- any threatening actions, incidents or behaviour they have or are alleged to have committed.

The information relating to the creation and sharing of a 'flag' needs to be handled carefully taking into account security and confidentiality concerns. Corporate standards for recording and investigating incidents that could result in the application of a flag need to be followed consistently and it is essential that information that needs to be shared with staff or sub-contractors to minimise risk is done so appropriately and efficiently. This means personal data, and often sensitive personal data, will be included in a risk marker and so must comply with the Data Protection Act 1998 (the Act). As such, access to information about risk markers will need to be restricted and appropriate steps should be taken to ensure that the information is secure and any access granted reflects a genuine need to view the information.

For the processing of this personal data to be fair, the Data Controller should normally inform individuals who have been identified as being a potential risk soon after a decision has been made to add a marker to their record. It should be part of

the procedure to write to the individual setting out why their behaviour was unacceptable and how this has led to the marker.

The individual should be told:

- the nature of the threat or incident that led to the marker;
- that their records will show the marker;
- who you may pass this information to; and
- when you will remove the marker or review the decision to add the marker.

There may be extreme cases where informing the individual would in itself create a substantial risk of a violent reaction from them, for example, because of the nature of the incident or the risk to another individual. In these cases it may not be sensible to inform the individual as described.

If this is the case, the Data Controller must be able to show why they believe that by informing the individual of the marker there would be a substantial risk of further threatening behaviour.

You should make all decisions on a case-by-case basis and keep records.

A more detailed guidance note on the creation, use and sharing of risk markers is currently being developed to ensure that the Council has a consistent approach to the use of this information.

11. Shielded Records

Shielded Records refer to the records of a customer who is at risk of physical or verbal harm in some way. There are many examples of why a customer could be at such a risk. Example include: known victim of abuse or domestic violence, at risk from honour crime, on the witness protection register, on the sex offenders register etc.

Shielding refers to the withholding of the whereabouts and contact details of an individual and is only applied where there are strong reasons to do so, for example, where a practitioner has reason to believe in their professional opinion that not doing so is likely to, for example:

- place a child at increased risk of significant harm;
- put a child's placement at risk (in the case of adoption);
- place an adult at risk of serious harm: and/or
- prejudice the prevention of a serious crime.

A more detailed guidance note on the creation, use and sharing of shielded records is currently being developed to ensure that the Council has a consistent approach to the use of this information.

12. Training

12.1 Training

It is the Council's Policy that all employees who hold or process personal data receive the appropriate training in order to comply with the Data Protection Act 1998.

Data Protection training is a crucial element of staff awareness. Council staff need to be aware of their obligations relating to any personal data they process as part of their Council duties. Failure to adhere to the eight data protection principles can lead to serious problems and prosecution.

Directorate contacts provide training in this area as well as a half-day training session being available through Central Training department of the Resources directorate. [For further details of training please contact your directorate representative or the Corporate Information Governance Team].

13. Security

13.1 The nature of information and its security

Birmingham City Council is committed to implementing BC ISO/IEC 17799: 2005 Code of good practice for information Security Management. This standard is minimum benchmark required by the Data Protection Act.

There are three key points we need to understand and have clearly in mind when thinking about information security.

“Information exists in many forms; printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films or spoken in conversation.”

“Information Security management is a combination of management and technological process.”

“We all have a part to play in making sure that our information assets are safe”

More information can be found in the Information Security Policy and a practical guide to implementation is available in the form of the Information Security Implementation Toolkit, both available on In-line.

14. Framework Code of Practice on Information Sharing

In 2007 the Information Commissioners Office issued its Framework Code of Practice guidance on information sharing. The aim of the code was to help organisations adopt good practice when sharing information and comply with the Data Protection Act 1998. The Council have adopted this approach and produced a Framework Code of Practice on Information Sharing, which is available as part of the guidance documents linked to this policy

15. Data Protection Guidance

Guidance Note 1 - Subject Access > Sections 7 to 9 of the Act gives individuals the right to request personal data relating to themselves the 'data subject'. Once received a data controller needs to respond within 40 calendar days of receipt of the written request from the individual concerned.

Guidance Note 2 - The Data Protection Principles > the principles are the foundation on which the Act is set and data controllers need to comply with these principles in order to satisfy the legal requirements set out by the legislation.

Guidance Note 3 - The Exemptions > There are a number of exemptions within the Act and this guidance outlines what they are and when they can be relied upon.

Guidance Note 4 - Disclosures > All data controllers processing personal data need to be aware of the correct procedure in terms of disclosing the data 'fairly & lawfully'

Guidance Note 5 - Notification > the Information Commissioner keeps an entry of all data controllers who process personal data for a number of different purposes. The register is available for anyone to view and can be located via the Information Commissioner's web-site.

Guidance Note 6 - Fair Processing of Personal Data > The 1st data protection principle states that "*Personal data shall be processed fairly & lawfully*". This guidance details how to go about collecting personal and sensitive data about individuals and gives examples of statements that can be used on data collection forms.

Guidance Note 7 - Seventh Principle > The 7th principle states that "*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*" This guidance explains in further detail the principle itself and other relevant information relating to security of personal data.

Guidance Note 8 - Data Matching > Data matching is the computerised comparison of two or more sets of records with the main objective of searching for records relating to the same individual.

Guidance Note 9 – Framework Code of Practice > The scope of this Framework Code of Practice is to support 'information sharing' requirements, when sharing personal data, to ensure compliance with the Data Protection Act 1998 ("DPA") and other relevant legislation regarding the use, collection and storage of personal information across Birmingham City Council.

Guidance Note 10 – Use of children's data > The Information Commissioner's guidance suggests that children from the age of 12 will have the capacity to give valid informed consent for the processing of their personal data. This will include exercising Subject Access Rights under section 7 of the Data Protection Act.

16. Related Guidance

Further related guidance on information management / security / governance can be found on the Council's Policies, Standards, Procedures and Guidelines database.

17. Compliance - Related Legislation

17.1 Links to other associated legislation

The Freedom of Information Act 2000
The Children Act 2004
The Disability Discrimination Act 2005
The Human Rights Act 1998
The Environmental Information Regulations 2004
The Copyright, Patents and Design Act 1988
The Computer Misuse Act 1990
The Defamation Act 1996
The Electronic Communications Act 2000
The Regulation of Investigatory Powers Act 2000
The Re-Use of Public Sector Information Regulations 2005
The Civil Contingencies Act 2004
The Criminal Justice and Immigration Act 2008

18. Definitions

Data > Any information automatically processed or going to be automatically processed. This includes information contained within structured and unstructured manual files.

Personal Data > Information relating to a living identifiable individual

Sensitive Personal Data > Information relating to an individual's race/ethnic origin, their political opinions, religion, trade union membership, health, sexual life, criminal or alleged offences.

Data Controller > Person (i.e. natural person or legal body such as a business or public authority) Decides manner in which, and purpose for which, personal data are processed.

Data Subject > An individual who is the subject of the personal data/information

Data Processor > A person who processes of behalf of the data controller under instruction

Processing > any activity/operation performed on personal data - whether held electronically or manually, such as obtaining, recording, holding, disseminating or making available the data, or carrying out any operation on the data. This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. **It is difficult to envisage any activity, which does not amount to processing.**

Information Commissioner > an independent Officer appointed by Her Majesty the Queen and who reports directly to Parliament.