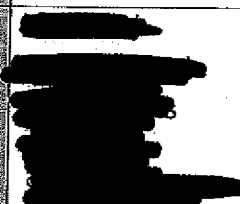




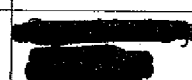






Barnet Partnerships Information Sharing Protocol

London Borough of Barnet

Document Control

| | | | |
|-----------------------------|--|-----------|------|
| Document Description | Barnet Partnerships Information Sharing Protocol This document forms the framework of all LBB and Partner Data Sharing Agreements and should be read in conjunction with the specific Agreements | | |
| Version | V7.2 | | |
| Date Created | July 2011 | | |
| Status | Draft | | |
| Authorisation | Name | Signature | Date |
| Prepared By: |  | | |
| Checked By | | | |

Version Control

| Version number | Date | Author | Reason for New Version |
|----------------|--------------|---|--|
| V1.0 | Dec 2010 |  | Initial draft |
| V2.0 | June 2011 |  | Redrafted and expanded. Incorporation of ICO guidance and legal requirements |
| V3.0 | June 2011 |  | Further expansion and comments |
| V4.0 | Aug 2011 |  | Amalgamated with the current personal data sharing protocol to create one overarching council protocol |
| V5.0 | Aug 2011 |  | Further amendment and comment |
| V6.0 | Sept 2011 |  | Further amendment |
| V7.0 | January 2012 |  | Additional comments |
| V7.1 | June 2012 |  | Comments incorporated |
| V7.2 | July 2012 |  | Circulated to IGC members, addition to FOI section accepted. |

Date last reviewed: June 2012
Date of next review: June 2013

Contents

| | | |
|----|--|----|
| 1 | Introduction..... | 1 |
| | 1.1 The need to share information between partner organisations | 1 |
| | 1.2 The need for an Information Sharing Protocol | 1 |
| 2 | Aims and Objective..... | 1 |
| 3 | Purpose and Scope | 2 |
| 4 | Associated legislation and guidance..... | 3 |
| 5 | Partner Organisations..... | 3 |
| 6 | Roles and responsibilities | 4 |
| | 6.1 Notification with the Information Commissioners Office (ICO) | 4 |
| | 6.2 Governance Group | 4 |
| | 6.3 Caldicott Guardian | 5 |
| | 6.4 Employees | 5 |
| 7 | Types of Information | 5 |
| | 7.1 Level 1 – Non-Personal / Open Data | 5 |
| | 7.2 Level 2 – Non-Personal / Depersonalised Data | 6 |
| | 7.3 Level 3 – Personal Data..... | 6 |
| 8 | How to share | 7 |
| | 8.1 Need to know basis..... | 7 |
| | 8.2 Data quality | 7 |
| | 8.3 Access to information..... | 8 |
| | 8.4 Consent | 8 |
| | 8.6 Security..... | 9 |
| | 8.7 Data Retention | 9 |
| | 8.8 Staff Awareness / Training..... | 9 |
| 9 | Duty of confidentiality | 10 |
| 10 | The Human Rights Act 1998..... | 10 |
| 11 | Freedom of Information Act 2000 | 11 |
| 12 | Subject Access and Access to Information..... | 12 |
| 13 | Management of the Protocol..... | 13 |
| | 13.1 Reviewing the Protocol | 13 |
| | 13.2 Monitoring of Individual Sharing Agreements | 13 |
| 14 | Complaints..... | 14 |
| 15 | Undertaking / Agreement..... | 14 |
| 16 | Signatories..... | 14 |
| 17 | Appendix A - Data Protection Legislation | 15 |

1 Introduction

1.1 The need to share information between partner organisations

Whilst public authorities must safeguard the information they hold, often the needs of the public are best served by the sharing of information between public sector partner agencies where it is appropriate to do so.

Sometimes it is only when information held by different agencies is pulled together that a person is seen to be in need of additional or alternative services. Sharing information, therefore, is a key element to the delivery of high quality, cost effective and seamless public services.

The Data Protection Act 1998 (DPA) places an emphasis on protecting privacy which has, in the past, made organisations reluctant to share information. The balance needed in order to share information for the purpose of providing an efficient and effective service and that of ensuring the protection and privacy of individuals is one that needs to be appropriately managed.

1.2 The need for an Information Sharing Protocol

It is necessary that all partners concerned have a clearly defined framework to facilitate the sharing of personal data whilst respecting the rights of the individuals.

The purpose of this framework is to facilitate the exchange of information between local public services effectively, fairly and lawfully and to provide a single, managed, clear joint approach to exchanging information.

2 Aims and Objective

This protocol aims to provide a clear, robust framework for the secure and legal sharing of information between Partner Organisations. It:

- clarifies the legal basis on which information can be shared
- clarifies partner responsibilities
- provides a framework within which organisations can develop individual Information Sharing Agreements specific to their service need
- establishes a common set of principles under which information will be shared
- encourages flow of data
- sets out the processes by which information will be exchanged, monitored and managed
- protects the rights of individuals
- encourages transparency through release of data

It is important that we meet both statutory obligations and the needs and expectations of our customers; assisting both professionals and public to feel confident that personal data is being shared in the right ways for the right reasons.

The purposes for which information sharing is to be undertaken are: -

- Provision of appropriate care services
- Improving the health of people in the local community
- Protecting people and communities
- Supporting people in need
- Investigating complaints
- Managing and planning services
- Commissioning and contracting services
- Developing inter-agency strategies
- Performance management and audit
- Research
- Staff management and protection
- Prevention of Crime and Disorder

The protocol outlines three levels of data sensitivity and an agreed set of principles under which information will be shared and used:¹

| | |
|---------|--------------------------|
| Level 1 | Non-Personal / Open Data |
| Level 2 | Non-Personal / Protected |
| Level 3 | Restricted |

3 Purpose and Scope

- For the purpose of this protocol the term “data” and “information” are interchangeable.
- This Sharing Protocol will act as an overarching document which will be underpinned by Individual Information Sharing Agreements specific to service areas and partner organisations
- Each underpinning Information Sharing Agreement will set out the detailed arrangements relevant to that particular sharing arrangement and all Agreements will need to be compliant with this Protocol and must be based on the Information Sharing Agreement Template (Appendix A).
- Whilst not contractually binding, this Protocol sets out good practice and standards to ensure compliance with partners’ legal responsibilities governing the sharing of personal data

¹ Indicative classification, may be different depending on organisations protective marking schema, although it is expected that there will only be 3 distinct levels of classification.

4 Associated legislation and guidance

The collection, use and sharing of information (including personal data) may be governed by a number of different areas of law and guidance including:

- The Data Protection Act 1998
- The Access to Health Records Act 1990
- The common law duty of confidentiality and tort of breach of confidence
- The Crime and Disorder Act 1998
- The Criminal Procedures and Investigations Act 1996
- The Environmental Information Regulations 2004
- The Freedom of Information Act 2000
- The Human Rights Act 1998]
- European Union law
- Caldicott guidelines
- The Regulation of Investigatory Powers Act 2000
- The law the governs the actions of public bodies (administrative law)
- Code of Recommended Practice for Local Authorities on Data Transparency

Before entering any information sharing agreements under this protocol Partner Organisations must:

- a. Establish whether there is power to carry out the function to which the information sharing relates.
- b. Check whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.
- c. Decide whether the sharing of the data would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim and unnecessary in a democratic society.
- d. Decide whether the sharing of the data would breach any obligations of confidence.
- e. Decide whether the data sharing would be in accordance with the Data Protection Act 1998, in particular the Data Protection Principles

5 Partner Organisations

By signing up to this Protocol, all partner organisations are making a commitment to:

- adhere to the provisions laid out in of this Protocol
- demonstrate a commitment to achieving the appropriate compliance with the DPA and other associated legislation
- show a willingness and commitment to sharing

- facilitate the exchange of information where necessary to promote good quality and well targeted public services
- ensure that they and all relevant staff are aware of and comply with their responsibilities in relation to: (a) this Protocol, (b) information sharing agreements they enter into under this protocol and (c) any procedures or guidance issued with regards to information sharing by their own organisation, local partners and national bodies.

It is envisaged that this framework will evolve and develop over time, especially as new members join the Partnership.

6 Roles and responsibilities

Each Partner Organisation will nominate a Governance Group / Group of Senior Officers as appropriate that will be responsible for managing the information exchanges within their organisation

6.1 Notification with the Information Commissioners Office (ICO)

The Act requires all organisations that process personal data to make a formal notification of its processing to the Information Commissioner. It is particularly important when engaging in information sharing that the purposes for which the data are to be used are included in the notification – if the notification is incomplete in any way appropriate amendments must be submitted before processing can start.

6.2 Governance Group

Each Governance Group will:

- ensure that their organisation has an up-to-date and accurate data protection notification (as reference in section 8.1) registered with the Information Commissioner which allows for the collection, use and transfer of the data to be shared
- develop systems of implementation, dissemination, guidance, training and monitoring to ensure that this framework is known, understood and followed by all employees and contractors who need to share information
- Promote good practice in the sharing of personal data by ensuring compliance with the principles, purposes and processes of this framework
- be responsible for agreeing and signing information sharing agreements under this protocol
- maintain a register of information sharing agreements made under this protocol

The names and contact details of the officers who sit on the Governance Group are set out in Section 18 of this protocol. This list shall be shared

freely between Partner Organisations, along with any updates or changes that may from time to time occur.

6.3 Caldicott Guardian

All NHS and Social Care organisations (including the London Borough of Barnet) **must** appoint a Caldicott Guardian who will act as the 'gatekeeper' of service users' information.

All Partner Organisations recognise the requirements that Caldicott imposes on NHS organisations and social services departments. They will ensure requests for information from these organisations are dealt with in a manner compatible with these requirements.

6.4 Employees

Every employee working for a Partner Organisation:

- is personally responsible for the safekeeping of information they obtain, hold, use or disclose in the course of their job
- should have a suitable level of awareness and training in how to obtain, use and share information appropriately, and
- must, before disclosing information under this protocol or any agreements under it, take any necessary steps to ascertain the identity and authority of any intended recipient of that information.

7 Types of Information

7.1 Level 1 – Non-Personal / Open Data

Following central government's drive to make the public sector more transparent to citizens, Partner Organisations should pro-actively publish as much information as possible. Once information has been identified as Level 1, the expectation is that Partner Organisations will make this information publicly available.

Level 1 information is information that:

- does not identify specific individuals, either by itself or in addition to other information in the public domain
- does not fall under any exemptions or exceptions in the Freedom of Information Act 2000 and Environmental Information Regulations 2004
- is not subject to a formal information sharing agreement made under this protocol

7.2 Level 2 – Non-Personal / Depersonalised Data

Non-Personal or depersonalised information is information in a form where the identity of the individual can not be determined. i.e. you must ensure that:

- all identifiers and/or references which could lead to an individual being identified are removed
- the information being shared can not be combined with other information held by the partner organisation which in turn may result in the individual being identified

Level 2 information is not covered by the DPA and should be used where possible. Sharing between Partner Organisations should still be limited for the purposes of the enquiry.

- Commercially sensitive data is also categorised as Level 2. Commercially sensitive is defined in Section 43 of the Freedom of Information Act as a trade secret or where release of the information is likely to prejudice the commercial interests of any person. (A person may be an individual, a company, the public authority itself or any other legal entity.)

7.3 Level 3 – Personal Data

The sharing of personal and sensitive personal data is governed by the Data Protection Act 1998. Sharing personal and sensitive personal data is not an automatic assumption and there must be a clear purpose, for example achieving an objective or set of objectives that can only be achieved by way of sharing personal data.

The Data Protection Act 1998 defines 'personal data' as information relating to a living individual who can be identified either from that information or from that information in conjunction with other information that is in, or is likely to come into, the possession of the data controller

All partner organisations must agree that they may only share Level 3 data within the constraints of the following guidance: -

- The sharing of personal data is not permitted where the sharing of depersonalised data would serve the same purpose.
- A person's full name is an obvious likely identifier; but other information such as a customer reference number, address, photograph or CCTV image could also identify them
- The Partnership need to consider whether the sharing of personal and sensitive personal data is absolutely necessary in order to achieve their

objective, For example, can the objective be achieved by sharing anonymised data.

- Level 3 information will be shared on a case by case basis and where it is necessary for information to be shared. Personal data will be shared only on a need-to-know basis
- Personal data will only be shared when the disclosing partner is satisfied that the sharing complies with the Data Protection Act 1998 and the Human Rights Act 1998
- Partner Organisations should only share Level 3 information with one another under agreed and signed information sharing agreements drafted in accordance with an approved Template (as attached as Appendix) and ICO guidance

8 How to share

The sharing of information within the Partner Organisations will be based on the following key principles: -

8.1 Need to know basis

- Information sharing must have a clear objective or set of objectives
- Where it is agreed necessary for information to be shared, this will be done on a “need-to-know” basis only i.e. the minimum information consistent with the purpose for sharing will be given.
- Partner Organisations will use personal information disclosed to them under an agreement only for the specific purposes set out in the agreement. Information disclosed will not be regarded by that organisation as information for the general use of the organisation.
- Restrictions may also apply to any further use of non-personal data, such as commercial sensitivity or prejudice to others caused by the information released, and this should be borne in mind when considering secondary use for non-personal data. If in doubt the information's original owner should be consulted

8.2 Data quality

- Data quality needs to be of a standard fit for the purpose the information is to be used for, including being complete, relevant, reliable, valid, accurate and as up to date as required for the purposes for which it is being shared. Without this any decision made on the information may be flawed and inappropriate actions may result.

- Steps must be taken to validate information, such as checking with the person who originally provided the information, if you are in any doubt as to its accuracy.
- If the individual has informed the organisation that, in their view, the information is inaccurate, then a record should be made on the file that they have expressed this view. Where such information has been shared with other organisations, they must be made aware of any actions taken in respect of inaccuracies or corrections made.
- If any member of staff records information either in writing or in an electronic format, the source of the information must also be clearly recorded as well as whether or not it is an opinion or factual observation.
- Partner Organisations are expected to ensure that the Personal Data and Sensitive Personal Data that it holds is processed in accordance with DPA principles: this includes ensuring that the Data is accurate, complete and up-to-date and is not kept any longer than is necessary.

8.3 Access to information

- Appropriate access procedures and controls must be agreed to limit the right to access the shared personal data to those who require it
- Where information is shared with individual's consent, the data will be seen as being under the control of the party the information was shared with and they are responsible for any further sharing or use of it
- Where information is not shared by consent of the individual, this information will remain under the control of the originating Data Controller and they will need to determine any further sharing or use with any other third parties.

8.4 Consent

Wherever possible, organisations should seek to obtain consent from the service user to share their personal data (Level 3 information). Where consent to disclose information is requested, the service user will be made fully aware of the information it is proposed to share and the purposes for which it will be used.

If a person is unwilling to give consent, information will only be shared where there are appropriate statutory grounds for doing so

The data subject will have the right to withdraw consent at any time and should be informed of this right. Partner Organisations must ensure

procedures are in place for ensuring that a written record is kept of consent given or withdrawn.

8.5 Sharing without consent

Organisations must document any decisions to share personal data without consent and these decisions must show how they comply with the requirements of the relevant legislation.

8.6 Security

- Each Partner Organisation must have achieved or will be working towards ISO 27001, the International Standard for Information Security Management, or have met or shown to be working towards a similar level of compatible security. Partner Organisations should ensure that the minimum standards of security, that they require, is agreed with Partner Organisations with whom their information will be shared and included in the information sharing agreement.
- Partner organisations are to agree standard procedures to facilitate the exchange of information in a secure method reflective of the information being shared. Where a partner has specific security requirements, for example a corporate policy, these policies should be made available to other Partner Organisations. This will assist in ensuring the agreed level of standards when entering into a new ISA.

8.7 Data Retention

- The fifth data protection principle in the DPA states that personal data shall not be kept for longer than is necessary for the purpose or purposes for which it is processed.
- Organisations must ensure they have appropriate retention schedules in place which are adhered to along with any statutory requirements. Where no provision has been made best practice must be applied and the retention scheduled updated accordingly.

8.8 Staff Awareness / Training

Partner Organisations will ensure that all of their staff involved in information sharing are aware of and compliant with their responsibilities in relation to this Protocol. They must have an appropriate level of knowledge of the contents of this Protocol, plus any additional requirements of their own organisation, to take responsibility for agreeing such disclosures.

9 Duty of confidentiality

All Partners should be aware that they are subject to a Common Law Duty of Confidentiality, and must adhere to this.

"In Confidence" information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular where a professional relationship may exist e.g. doctor/patient, social worker/client; lawyer/client etc.

The duty of confidence only applies to person identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.

There are generally three categories of exception to the duty of confidence:

- where there is a legal compulsion to disclose
- where there is an overriding duty to the public, and
- where the individual or organisation to whom the duty is owed has consented to disclosure.

The guidance from the Information Commissioner states that because such decisions to disclose 'in the public interest' involve the exercise of judgement it is important that they are taken at an appropriate level and that procedures are developed for taking those decisions.

10 The Human Rights Act 1998

The Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law be compatible with the Convention Articles and places a legal obligation on all public authorities to act in a manner compatible with the convention. Should a public authority fail to act in such a manner then legal action can be taken under Section 7 of the Act.

Article 8 of the Act states that:

"Everyone has the right to respect for his private and family life, his home and his correspondence..."

The Act further states that this is not an absolute right and acknowledges that under certain conditions this right can be lawfully overridden.

11 Freedom of Information Act 2000

LBB are committed to being open and transparent in providing information to the public. Publication of 'level 1' data (as defined in section 2) wherever possible is a mechanism to assist in meeting our commitment. Our partner organisations are encouraged to use a similar approach where possible

Under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) Partner Organisations may be obliged to publicly disclose information on their records. This may include information a Partner Organisation has received under an agreement made pursuant to this protocol.

It is for the Partner Organisation in receipt of a request under the FOIA to decide how it responds, including deciding whether any of the exemptions to disclosure apply. In reaching this decision Partner Organisations may need to consult affected third parties, including the other Partner Organisations signed up to this protocol, for their views on the request.

When deciding whether it is necessary to consult third parties, Partner Organisations will be guided by the code of practice issued under section 45 of the FOIA. Whilst views of third parties should be taken into account, it is ultimately for the Partner Organisation in receipt of a request to decide how it shall respond.

The Code of Recommended Practice for Local Authorities for Data Transparency requires the Council, and Partner Organisations, to understand what they hold, what their communities want and then release it in a way that allows the public, developers or the media to use.

The FOIA requires local authorities to operate a publication scheme approved by the Information Commissioner's Office that sets out information that must be routinely published. Partner Organisations will need to provide information for the purposes of complying with the requirements of the publication scheme.

Local authorities should build and maintain an inventory of the public data that they hold so that people are able to know what is available to them. If public data would be released under Freedom of Information it should be included in the inventory. Partner Organisations may need to contribute to the inventory list compiled by the Council.

There are minimum levels of data that the Council is required to publish, in accordance with The Code of Recommended Practice for Local Authorities for Data Transparency:

- Expenditure over £500, (including costs, supplier and transaction information). Any sole trader or body acting in a business capacity in receipt of payments of at least £500 of public money should expect such payments to be transparent.

- Senior employee salaries, names (with the option for individuals to refuse to consent for their name to be published), job descriptions, responsibilities, budgets and numbers of staff. 'Senior employee salaries' is defined as all salaries which are £58,200 and above (irrespective of post), which is the Senior Civil Service minimum pay band. Budgets should include the overall salary cost of staff reporting to each senior employee.
- An organisational chart of the staff structure of the local authority including salary bands and details of currently vacant posts.
- The 'pay multiple' – the ratio between the highest paid salary and the median average salary of the whole of the authority's workforce.
- Members' allowances and expenses.
- Copies of contracts and tenders to businesses and to the voluntary community and social enterprise sector.
- Grants to the voluntary community and social enterprise sector should be clearly itemised and listed.
- Policies, performance, external audits and key inspections and key indicators on the authorities' fiscal and financial position.
- The location of public land and building assets and key attribute information that is normally recorded on asset registers
- Data of democratic running of the local authority including the constitution, election results, committee minutes, decision - making processes and records of decisions.

12 Subject Access and Access to Information

Under the sixth data protection principle personal data must be processed in accordance with the rights of data subjects set out in the DPA.

This includes the right of any individual to be provided access to any information held about them by a Partner Organisation, whether on computer or manual files. This includes a right to be given details of the purposes for which their personal data is held, from whom it was obtained, and to whom it is or may be disclosed. This right, known as the right of subject access, is subject to a limited range of exemptions.

Partner Organisations must have appropriate procedures in place to regards to the handling of Subject Access Requests and staff must be appropriately trained in how to handle requests in line with legislation.

13 Management of the Protocol

The Partner Organisations that are signatories to a protocol have responsibility for:

- Ownership of the Protocol
- Approving the content of Protocol
- Ensuring dissemination of the Protocol
- Agreeing and arranging training as required on the Protocol
- Implementation the requirements of the Protocol within their organisation
- Monitoring implementation and compliance of the Protocol
- Reviewing and recommending any changes to the Protocol

13.1 Reviewing the Protocol

The protocol will be subject to a formal review process annually to be instigated and managed by the responsible Corporate Governance Group/function.

Any changes to the contents will be formally approved and adopted following consultation and agreement with signatories of the Protocol.

All staff responsible for information sharing under this Protocol will be informed of any changes. Training (where necessary) will be undertaken. All documentation will be amended and version controlled.

13.2 Monitoring of Individual Sharing Agreements

All Partner Organisations must implement and communicate a procedure for monitoring individual Sharing Agreements. Periodic reviews must be undertaken to assess whether the stated objectives have been determined etc. Individual Sharing Agreement should be amended and agreed to reflect any changes required following the review.

Partner Organisations must identify and log incidents in relation to individual Sharing Agreements which highlight any non-compliance.

The following incidents will be logged and reported:

- Refusal to disclose information and reasons for refusal
- Conditions being placed on disclosure
- Delays in responding to requests for information (FOI and SAR)
- Disclosure of information to members of staff who do not have a legitimate "need to know"
- Inappropriate or inadequate use of the procedures
- Disregard of the Protocol and agreed security procedures

- Use or disclosure of personal data for purposes other than those agreed in the specific Information Sharing Agreement
- In the case of shared databases, actual or suspected breach

Non-compliance by a Partner Organisation will be reported to that organisation's data protection officer. Instances of a DPA breach must be dealt with promptly and in line with ICO guidance. Further details of how breaches will be handled should be provided in the specific Data Sharing Agreement.

14 Complaints

The Partnership must be committed to having procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal data. Received from both staff and members of the public.. Further details of how complaints will be handled should be provided in the specific Data Sharing Agreement.

15 Undertaking / Agreement

The signatories to the protocol agreed to accept the procedures laid down in the document and are committed to providing a secure framework for sharing personal data between their agencies in a manner compliant with their statutory and professional responsibilities.

16 Signatories

| Authority / Organisation being represented | Name of Responsible Officer | Signature | Date |
|--|-----------------------------|-----------|------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

17 Appendix A - Data Protection Legislation

The key piece of legislation governing the collection and use of personal data is the **Data Protection Act 1998** (the DPA).

The term “personal data” is defined in the DPA as:

data which relate to a living individual who can be identified;

- (a) from those data, or
- (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

The DPA both:

- grants rights to individuals (data subjects) in respect of their personal data and
- obliges those that process (e.g. collect, hold and use) personal data to do so in accordance with a set of data protection principles contained within the Act.

Rights of individuals

The DPA gives seven rights to individuals in respect of their personal data held by others. They are:

1. The right of subject access
2. The right to prevent processing likely to cause unwarranted substantial damage or distress
3. The right to prevent processing for the purpose of direct marketing
4. Rights in relation to automated decision taking
5. The right to take action for compensation if the individual suffers damage
6. The right to take action to rectify, block, erase or destroy inaccurate data
7. The right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the DPA has been contravened.

Data Protection principles

The use of personal data is regulated by eight Data Protection Principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
 - i. at least one of the conditions in Schedule 2 is met, and
 - ii. 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 longer than is necessary for that purpose or 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.

Schedule 2 (first data protection principle)

The first data protection principle requires that at least one of the conditions in Schedule 2 of the DPA be met before personal data can be processed fairly and lawfully. These conditions are:

- (i) The Data Subject has given their consent to the processing
- (ii) The processing is necessary
 - for the performance of a contract to which the Data Subject is a party, or
 - for the taking of steps at the request of the Data Subject with a view to entering into a contract.

- (iii) The processing is necessary for compliance with any legal obligation to which the Data Controller is subject, other than an obligation imposed by contract
- (iv) The processing is necessary in order to protect the vital interests of the Data Subject
- (v) The processing is necessary
 - a. for the administration of justice
 - b. for the exercise of any functions conferred on any person by or under any enactment
 - c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
- (vi) The processing is necessary for the purposes of “legitimate interests” pursued by the Data Controller or by the third party or parties to whom the data are disclosed.

When applying condition (vi) you must further ensure that once you have established that there is a legitimate interest, these interests must be balanced against the interests of the individual(s) concerned. The “legitimate interests” condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. Your legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual’s legitimate interests will come first.

Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

Schedule 3 (first data protection principle)

When processing “sensitive personal data” the first data protection principle requires that at least one of the conditions in Schedule 3 of the DPA be met in addition to a Schedule 2 condition.

“Sensitive personal data” means personal data consisting of information as to:-

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The conditions in Schedule 3 DPA are:

- The Data Subject has given their “explicit” consent to the processing
- The processing is necessary to perform any legal right or obligations imposed on the organisation in connection with employment
- The processing is necessary to protect the vital interests of the individual or another person, where consent cannot be given by the individual, or the organisation cannot be reasonably expected to obtain consent or consent is being unreasonably withheld where it is necessary to protect the vital interests of another
- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject
- The processing is necessary in connection with legal proceedings, dealings with legal rights or taking legal advice
- The processing is necessary for the administration of justice or carrying out legal or public functions
- The processing is necessary for medical purposes