*Aim, Aspire, Achieve @ Abbeys*

# Abbeys Primary School

# Data Protection Policy

Abbeys Primary School
Melrose Avenue
Bletchley
Milton Keynes
(01908) 375230
Website: www.abbeysprimaryschool.org.uk
Email: abbeysprimary@milton-keynes.gov.uk

**Date adopted by the Governing Board:** **February 2018**
**To be reviewed:** **May 2018**

Last updated October 2015
Version 4

**Abbeys Primary School has adopted the Milton Keynes Council Data Protection Policy which is set out in the following pages.**

MILTON KEYNES COUNCIL

# Data Protection Policy And Code of Practice

## Table of Contents

# 1. Policy

This is a statement of the data protection policy adopted by Milton Keynes Council. It forms part of the Council's developing information management policy relating to The Data Protection Act 1998, the Human Rights Act 1998, Freedom of Information legislation, and the 'Modernising Local Government' strategy.

Milton Keynes Council needs to collect and use certain types of information about the people it deals with in order to operate. These include current, past and prospective employees, suppliers, clients, customers, and others with whom it communicates. In addition, the Council may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used - whether on paper, in a computer, or recorded on other material. There are safeguards to ensure this in the Data Protection Act 1998.

The Council regards the lawful and correct treatment of personal information as necessary both for successful operations, and to maintain confidence between the Council and those with whom we deal. We will ensure that the Council treats personal information lawfully and correctly. To this end we fully endorse and adhere to the Principles of data protection as laid out in the Data Protection Act 1998.

However, the Council wishes to encourage a climate of open and frank dealings with all members of the community. Where the Council holds personal information about any individual, the Council will endeavour to freely disclose that information to the individual concerned unless it could prejudice the rights of the individual concerned, the Council or any third party involved. Where this is the case, the Council will inform the individual concerned of the reason for refusal under the informal access provisions and will ask the individual to make a formal request in writing under the provisions of the Data Protection Act 1998. The Council will need to be satisfied about the identity of the individual. In the case of a child, the Council will also disclose information to the authorised parent or guardian. Access procedures are described in more detail in Section 3 below.

Specifically, the Principles require that personal information:

- shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
- shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

- shall be accurate and, where necessary kept up to date;

- shall not be kept for longer than is necessary for the purpose or those purposes;
- shall be processed in accordance with the rights of data subjects under the Act;
- Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- shall not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Therefore, Milton Keynes Council will, through appropriate management procedures and controls:

- fully observe conditions regarding the fair collection and use of personal information; meet its legal obligations to specify the purposes for which personal information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held, are able to be fully exercised under the Act. This includes the right to be informed that processing is being undertaken, the right of access to an individual's personal information, the right to prevent processing in certain circumstance and the right to correct, rectify, block or erase information which is regarded as incorrect;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

In addition, the Council will ensure that:

- there is someone with specific responsibility for data protection in the Council. Currently, the nominated data protection officer for the Council is Paul Wheeler, Head of IT Strategy;
- everyone managing and handling personal information understand that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;

- everyone managing and handling personal information is appropriately supervised;
- methods of handling personal information are clearly described;
- queries about handling personal information are promptly and courteously dealt with;
- anyone wanting to make enquiries about handling personal information knows how to do so;
- a regular audit and review is made of the way personal information is managed;
- our methods of handling personal information are assessed on a regular basis;
- our performance in handling personal information is reviewed and assessed on a regular basis.

The Data Protection Policy forms part of the Information Governance Policy Framework.

# 2. Code of Practice

## 2.1. Introduction

Data Protection is both good business practice and common sense. It deals with the integrity of information stored about living individuals; it ensures a reasonable degree of confidentiality about people and protects their privacy. It is not just about privacy, it ensures the reliability of information, and its fair and legitimate use by everyone concerned. The 1998 Act covers both manual and computerised records.. The definition of data, personal data and processing to encompass sound, images and paper records is very broad in definition. This has the effect of covering telecommunications as well as CCTV and other media, such as email and the Internet.

It encourages a climate of openness and transparency in the Council.

**Poor** record keeping leads to poor financial and operational control; bad relations with external bodies; lost business opportunities; poor employee relations and legal penalties.

**Good** practice is even more important when you are dealing with personal information. Clients, customers, employees, pupils, young people and their parents need to be confident that information about them is properly maintained.

Some of the circumstances when dealing with people may be sensitive for a variety of reasons, including legal or commercial reasons. People must be confident that information given in confidence will not be misused. Much of the 1998 Act has intentionally been left open to interpretation in order to cater for future advances in technology.

## 2.2. Data Protection Legislation

The European Data Protection Directive 95/46/EC is implemented into UK law in the form of the Data Protection Act 1998. It aims to give individuals in all EU member states the same rights regarding the use and storage of personal information held about them. The Data Protection Act 1998 received Royal Assent in July 1998 and was brought into force on 1 March 2000. The 1998 Act also brings together the access rights previously provided for under separate legislation, for example, the Access to Personal Files Act allowed individuals access to their own health, education, housing or social work files (now referred to as "accessible records" in the 1998 Act).

The Council is required to notify the Commissioner of our processing operations. This involves providing a description of the personal data we hold.

## The Eight Principles

The eight data protection principles are a fundamental component of the legislation. They prescribe acceptable conduct for the lawful management of personal information. They are the basic rules that control best practice and procedures. Ignore them and the Commissioner will intervene. A more serious contravention may eventually lead to an Enforcement Notice being served or a criminal prosecution. There are value judgements embedded in many areas of these Principles and it is for the Council to make decisions on, and treat personal information in a manner that can be fully justified and defended. The 1998 Data Protection Act requires that all these Principles must be observed. Failure to do so is a breach of the law.

### 2.2.1. First Principle Adherence

Personal data shall be processed fairly and lawfully and shall not be processed unless -

- at least one of the Schedule 2 conditions is met and in the case of sensitive data,
- at least one of Schedule 3 conditions is also met.
- The requirement to process the data fairly and lawfully is the overriding general condition. It will always be unlawful to process data if none of the conditions are met unless there is a specific exemption.
- Processing data is lawful when one of the Schedule 2 conditions are met.
- The data subject has given active "specific and informed" consent to the way their personal data is to be processed. Silence cannot be taken as consent.
- The processing is necessary for a contract with the data subject.
- The processing is necessary to comply with the Council's legal obligations.
- The processing is necessary to protect the vital interests of the data subject. Guidance given by the Commissioner is that this condition may only be employed in life and death situations.
- The processing is necessary for the administration of justice; for the exercise of statutory functions; for the exercise of the functions of government or other functions of a public nature exercised in the public interest (for example, those of a local authority).
- The processing is necessary for the purposes of the legitimate interests of the Council or third parties to whom the data is disclosed. This condition will not be available where the rights and freedoms or legitimate interest of the data subject make such processing unwarranted.
- However, even if at least one of the conditions is met, it may still be unlawful if, having regard to the wider circumstances, and any other relevant legislation, the processing is not fair or lawful. In addition, in considering the question of fairness, the courts and the Commissioner

will have regard to the "fair processing code". The code says that the method of obtaining personal data and whether there was any deception or anything misleading about the use or purposes to which the data would be put, is relevant to fairness. The code also specifies that where data or information is obtained from the data subject, the Council must, so far as is practicable, tell the data subject:

- Who the data controller is
- What the data is to be used for
- Any other information appropriate in the circumstances.

If the information is obtained from someone other than the data subject, these requirements are the same unless it would involve "disproportionate effort". Finally, if the data consists of information obtained from an organisation or person who is authorised or obliged by statute to provide the information, that data will always be treated as having been fairly obtained.

Sensitive Personal Data

Sensitive personal data is classed as information on racial or ethnic origin, political opinions, religious or other beliefs, trade union status, physical or mental health/condition, sexual life or any alleged offences or sentences.

In the case of sensitive data, at least one of following conditions

must also be met in order for processing to be regarded as being fair and lawful.

- The data subject has given their "explicit" consent to the particular processing of the sensitive personal data. A "blanket consent" will not suffice. The most obvious way of doing this would be to obtain the person's signature on a form with the relevant details printed there.
- The processing is necessary in connection with employment rights and obligations.
- The processing is necessary to protect the vital interests of the data subject where consent cannot be given or reasonably obtained. Again, this will normally only be in an emergency situation.
- The processing is necessary to protect the vital interests of another person and the data subject unreasonably refuses to consent.
- The processing is carried out by certain non-profit making bodies on its members' data.
- The information has been made public by the data subject
- The processing is necessary for legal proceedings, taking legal advice, or establishing, exercising or defending legal rights or for the administration of justice.
- The processing is necessary for the exercise of statutory or government functions.
- The processing is necessary for medical purposes.
- The processing is necessary for equal opportunities purposes, and there are safeguards for the rights and freedoms of the data subject.

- Any further Orders as specified by the Secretary of State.
- The Secretary of State has made an order specifying additional reasons for processing sensitive
- personal information without the explicit permission of the data subject for:
- prevention or detection of unlawful deeds
- confidential counselling and advice
- prevention and detection of incompetence or mismanagement
- some journalistic, artistic and literary purposes

While classed as sensitive for the purposes of the Data Protection Act, this does not preclude the need for due care and diligence in the use of other information normally regarded as sensitive, such as financial, legal and commercial information. People must be confident that information that they have given in confidence will not be misused. The requirement for fair collection and legitimacy of processing is discussed in more detail below.

### 2.2.2. Second Principle Adherence

Personal data shall be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. The legislation imposes a discipline on managers of personal information to be clear about the purpose for which they are collecting data. Having notified the Commissioner and the data subject of the purpose or purposes in collecting data to comply with the First Principle, activity must only be undertaken strictly within those purposes. For example, a local authority would not be entitled to tell a social work client that personal data was being taken for social work files and then pass it on the housing benefit section. Modern management practices and information may suggest innovative ways to use information gathered to enhance performance. In such cases, the new applications or procedures need to be notified to the Information Commissioner and the data subjects before they are implemented.

### 2.2.3. Third Principle Adherence

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. This principle obliges managers to apply purpose-related criteria to the amount and nature of information processed and requires judgement in individual circumstances. The critical question to be answered is, "How much information do I need to manage the operation properly?" The information must be adequate for the defined purpose. Too little information to carry out a purpose is as bad as too much. Incomplete information, though accurate, may be insufficient to allow proper processing. The data collected must also be easily identified as relevant for the intended purpose and should not be excessive.

Each decision will depend on the circumstances in the particular case but must be capable of being justified. For example, what may be irrelevant and excessive for payroll processing may be necessary for other employment purposes. Moreover, it may be necessary to hold different amounts of information for different people although it relates to the same purpose. Keeping a uniform amount of information simply for administrative convenience must be avoided. Simply collecting information just in case it may be useful is not acceptable. It is also wise to consider whether it is necessary to keep information about an identifiable individual for the activity or operation. You should depersonalise information whenever possible, while still achieving the specified objective.

### 2.2.4. Fourth Principle Adherence

Personal data shall be accurate and, where necessary, kept up to date. As in any process or operation, it is essential to use reliable data to perform the job properly. Without accurate data, the credibility and integrity of an operation can be compromised. In the case of personal data, there is the added risk of severely damaging an individual's interests and then being subject to litigation and penalties under the Act. Accuracy must be maintained, so updating of information is important in many cases. This does not just apply to current data. If historical data is retained for audit, research or other purposes, the information must also be accurate at the time that it was current. The difficulties in ensuring total accuracy are recognised, and a realistic approach is adopted in the Act by requiring the data controller to take reasonable steps to ensure the accuracy of information obtained from the data subject, or from a third party. Where there is disagreement about a matter of accuracy, then it is permissible to record the disagreement by annotating the data to indicate the data subject has challenged its accuracy.

### 2.2.5. Fifth Principle Adherence

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. This principle requires managers to consider how long information is retained and the justification for retaining the information. It must not be retained for longer than is necessary for the performance of its purpose. This may be a very short time, or in other circumstances it may be indefinite. It will depend on the data and its application. The Limitation Act 1980 is some guide to practice for some functions and operations. Codes of Conduct for professional bodies may specify other retention periods. In addition the Council's Records Management Policy & Data Retention schedules may provide additional guidance in this area. Information for research and historical purposes may be retained indefinitely.

### 2.2.6. Sixth Principle Adherence

Personal data shall be processed in accordance with the rights of data subjects under this Act. This principle makes the individual a fundamental part of the "system" of data protection, protecting his or her interests by exercising several important rights. These rights are explained in more detail in Section 2.6 , but in summary, they include the right to be informed that processing is being undertaken; the right to inspect personal data; the right to prevent processing in certain circumstances and the right to rectify, block or erase data. So, the Council's policies and procedures must be implemented to allow the rights of the data subject to be properly and fully exercised.

### 2.2.7. Seventh Principle Adherence

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. It is very important to remember that the definition of personal information includes both automated and manual records and that processing includes activities from the original collection of the information to its eventual destruction, so security must be viewed from a wide perspective. A judgement on what is necessary and appropriate is required. In determining reasonable security measures, managers will need to consider the sensitivity and value of the data, the risks to the data, both natural and man made, the cost of security and the consequences of compromising its integrity. This does not just relate to technology matter but also refers to the complete procedure for managing and operating with people, facilities and other agencies. This includes such issues as the employment and training of competent staff through appropriate employee management. The Act says, "The data controller must take reasonable steps to ensure the reliability of any employees…who have access to personal data" The Council and its officers are also responsible for ensuring that any agency operating on behalf of the Council as a data processor is able to ensure adequate security and is committed to do so under contract.

### 2.2.8. Eighth Principle Adherence

Personal data shall not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This Principle prevents the movement of personal information beyond the boundaries of the European Economic Area (EEA) unless that country demonstrates adequate data protection arrangements. Particular care must be taken when personal information is published on public facing web sites or sent by e-mail to ensure that informed consent is obtained from all individuals concerned. Council employees must not transfer personal information outside the EEA unless one of the conditions below apply:

- the data subject has given consent to the transfer
- the transfer is necessary as part of a contract between the data subject and the Council, or the transfer is necessary as part of a contract between the Council and a third party at the request of the data subject.
- there is a substantial public interest requirement
- the transfer is necessary as part of any legal proceedings
- Rights of Data Subjects
- the transfer is to obtain legal advice
- the transfer is to necessary to protect the vital interests of the data subject
- the transfer is part of a public register
- the transfer is approved or authorised by the Commissioner
- the transfer is by order of the Secretary of State.

- The EEA currently includes the 15 member states of the European Union plus Norway, Iceland and Liechtenstein.

## 2.3. Fair Collection & Legitimacy of Processing

The simple statement of the First Principle has wide-ranging implications. Processing is defined as obtaining, recording, holding, disclosing, and even disposing of personal information as well as carrying out a set of operations on it. So, the definition is very comprehensive. For processing to be fair, you must

- be candid and open in your dealings with data subjects about what the information is used for,
- your intentions, activities and the outcome regarding the use of information.

You will need to consider the audience for the information provided and use appropriate language. If you are dealing with children, you will need to give additional information. For information to be lawful, you must meet at least one of the **Schedule Two** conditions, and one of the **Schedule Three** conditions in the case of sensitive data, as well as complying with any other civil and criminal law. The Act also sets out a "Fair Obtaining Code". It requires that the Council makes certain information about processing activity available to the data subject at the time of obtaining any personal information directly from him, or when obtaining it from a third party, within a certain period unless it would involve "disproportion effort". Secondary legislation specifies safeguards and conditions that the Council has to comply with if a claim of "disproportionate effort" is made. The list of legitimising conditions, of which at least one must be met to comply with the first Principle, appears in Schedule 2. They include:

- the data subject consenting to the processing, or processing for various contractual or legal purposes; or,
- if 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, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject."

## 2.4. Sensitive Data

### 2.4.1. Equal Opportunities Monitoring

The first Data Protection Principle requires that in order for the Council to legally process sensitive personal information one of the Schedule 3 conditions must apply. The Act specifically allows processing relating to racial or ethnic origin, disability and religious or other beliefs for the purpose of equal opportunities monitoring. It is important that an individual completing a Council application form is not led to believe that providing information as to their ethnic origin etc. is a necessary part of claiming a particular benefit or service from the Council. The form should make it quite clear that the provision of the information is optional. Sensitive personal data as defined in the Act should never be used for additional purposes other than the ones originally stated when the information was collected.

The third Data Protection Principle also requires that personal data be adequate, relevant and not excessive in relation to the purpose for which it is held. If equal opportunities information was held as personal data, but is not used in practice, this would raise the question of relevance for the purpose it was collected.

### 2.4.2. Trade Union Membership

Trade union status is classified as sensitive personal information. So, particular care will need to be taken to ensure that unwarranted processing of trade union status does not take place. Normal processing for the purpose of payroll deductions will not cause any problems; nor will disclosure to the appropriate trade union as this is allowed under the Act. However, reports identifying the trade union status produced for management purposes will have to be closely monitored to ensure that their use is appropriate and justifiable under the Act, and that the individual's rights under the Act are protected. Care should be taken to ensure that non- membership of a trade union is treated with the same caution and sensitivity as information about membership of a particular trade union.

## *2.5. Rights of Data Subjects*

The Act contains a range of enhanced rights for data subjects. An individual is entitled to:

- be given access and be informed of personal data that is being processed relating to the individual.
- be given a description of the data
- be given any information as to the source of the data
- know the purpose for which the data is being processed
- know the recipient/s to whom they are or may be disclosed
- be informed of the logic behind any automated decision making
- have communicated to him/her, in an intelligible form, the information constituting any personal data of which the individual is the subject and to have communicated any information available to the Council as to the source of those data
- prevent processing of personal data where this may cause damage or distress
- prevent processing of personal data for direct marketing purposes
- seek compensation/judicial remedy for damage caused by the Council's failure to comply with the requirements of the Act

### 2.5.1. Subject Information Requests

When the Council receives a Subject Information Request in writing, the data subject is entitled to be informed whether personal information is being processes about them by the Council, or by a third party on behalf of the Council. The individual is also entitled to see, in a form that is understandable, all personal data held about them by the Council. For the purposes of the Act, any electronic request that can be retained for reference is considered a request in writing. Subsequent steps will need to be taken to confirm the identity of the person making the request.

The request should never be ignored just because there is insufficient information supplied initially. Where the data subject has not supplied sufficient information for the Council to identify whether it is holding information about the person, the Council is legally obliged to write to the individual explaining the position.

The data subject is also entitled to be given a description of the personal data, the purposes that it will be used for and any recipient or class of recipients that the data has been, or could be disclosed to. The data subject is also entitled to have a permanent copy of the personal information in an intelligible form unless the data subject waives this right or this involves "disproportionate effort" as well as a description of the logic involved in any automatic decision making procedure.

If the Council claims "disproportionate effort" then the data subject must still be allowed access to the data, and facilities made available to make requested data available in "permanent form".

Under the Act the data subject is entitled to be told the source of any data that the controller has obtained about the subject. This imposes an important obligation on Councils to record where they obtained personal data from if they have this data readily available. Councils also have an obligation to record where they pass personal data to, and to inform the data subject of this, too if requested.

The Council has 40 days to respond after receiving a request in writing, sufficient information to clearly identify the individual and the information requested, together with any fee as agreed by the Council, up to a maximum of £10 set out in the Act. It is important that reasonable steps should be taken to confirm the identity of the individual. The steps needed to identify the individual will vary depending on the sensitivity of the data to be released and the risk of releasing the data to anyone who is not entitled to it.

If supplying answers to the data subject is likely to identify another individual, the Council is entitled to delete that part of the data supplied unless the other individual has consented to this disclosure, or if it is not reasonable to delete the data. Even if the reference to the identity of the individual in question is deleted, the Council should still supply all remaining data to the data subject. Generally, all data on the data subject should be supplied wherever possible.

There are some exemptions to this where information is supplied by a doctor, for education or social work purposes. See Section 3 for more information.

Circumstances may arise where, when checking the data in response to a data subject's request, it is found the data is inaccurate or misleading in some way. There may be a temptation to amend it before passing it to the data subject. Data must not be amended before being supplied or deleted unless it was going to be amended or deleted anyway.

The data subject is entitled to make as many requests as he or she likes, as often as he or she likes, but a reasonable time must elapse between requests.

The right of access to personal data can be enforced by court order.

### 2.5.2. Disproportionate Effort

The Act gives scope for the Council to decline to provide a copy of personal data in permanent form if the data subject agrees to this, or if supplying it would require "disproportionate effort". This might apply if the printed version of the data is very long and/or has to be retrieved from a remote archive. The data subject is still entitled to the data. However, he or she may not be able to walk away with a copy if the disproportionate effort issue arises. In other words, the Council cannot withhold personal data on a data subject on the grounds of disproportionate effort. All the Council can withhold is the data in a particular permanent form. The Council may be unable to supply a copy in permanent form, but must offer to supply the data in another form.

The Act does not clarify what other methods are allowed, but one method would be to invite the data subject to inspect the files for him or herself and supply facilities for the individual to copy a sub-set of the information required. The Council is still obliged to ensure that information relating to third parties or unrelated business activities is not inadvertently disclosed to the individual concerned. The Commissioner has stated that she takes a pragmatic approach to the question of disproportionate effort of making permanent copies. The intention is to balance the rights of the data subject and the Council.

Where the Council declines to provide a copy of the data in permanent form, the Act requires the Council to record the justification for claiming disproportionate effort in writing.

### 2.5.3. Subject Information Notice

The Data Protection Act sets out the information that has to be given to a data subject either at the time of collection or when information is received from a third party. The subject information notice has to be given regardless of whether the data have been obtained from the data subject or from the third party.

<u>Fairness in process</u>

Whichever condition is satisfied for processing personal data, the data controller must ensure that the processing is fair. This means that when obtaining data from a data subject, then you must ensure that the following information is made readily available:

- the identity of the Council
- the identity of any nominated representative for the purposes of the Act
- the purpose or purposes for which the data is intended to be processed, and
- any other information necessary to ensure fairness: such as the likely consequences of the processing, and whether they envisage the data being disclosed to a third party.

In many cases where personal data are obtained from someone other than the data subject, the data controller must provide the above information to the data subject. There are very limited exceptions from the fair processing code, but these do not absolve you from the overriding duty to process personal data fairly and lawfully.

The case for consent

So long as there is no likelihood of a significant adverse effect on the individual through processing their information, the specific consent of the data subject will not always be required. Where consent needs to be sought, the data subject should be left in no doubt that they are giving their consent - consent should be specific and informed. It cannot be inferred from non-response to a request or communication between a data controller and individual, nor can consent be deemed valid if given under duress or because of misleading information.

Even where consent has previously been given, then you cannot assume that this will endure forever, and individuals must be allowed to withdraw consent at anytime after it is provided. In many cases the data controller may not need to provide individuals with too much detail in order to ensure that he or she is informed (for example when providing address details for a newspaper delivery). In others, nothing less than clear written consent will be required. Here the individual will need to be assured that they are fully informed of the details of the purposes for which the information is being collected, the length of time it will be retained and any third parties to whom the information will be disclosed. When consent is being sought for processing sensitive data, explicit consent is required. This means that the individual is absolutely clear about the detail of the processing. This should include the type of data and information to be processed, the reasons for processing and any part of the processing which may have an effect on the individual (for example any parties to whom the data or information are disclosed).

Milton Keynes Council - Standard notice

***In order to provide services to you, we need to record your details, which you have a right to see and check. Information may be shared with organisations we work with to provide services to you. We will process and safeguard your details in accordance with the Data Protection Act.***

***Information may also be used in connection with the prevention and detection of crime and fraud and for planning, statistical and research purposes.***

### 2.5.4. Prevention of Processing

The data subject is entitled to submit a notice in writing at any time to prevent within a reasonable time any processing that is causing, or is likely to cause unwarranted and substantial damage or distress to either themselves or other named individuals. The Council must establish procedures to process these data subject notices and respond to the data subject within 21 days of receiving the notice. The response must contain a statement on how the Council has complied or intends to comply with the notice, or the reasons for regarding the notice as unjustified. The data subject cannot exercise this right if:

- The data subject has given consent to the processing. This could be verbal, although it is best to record it.
- If the processing is necessary for the performance of or entering into a contract to which the data subject is a party.
- If the Council is legally obliged to do the processing
- If the processing is necessary to protect the vital interests of the data subject.

### 2.5.5. Automated Decision Making

The data subject is entitled to know if the Council is processing data about him or her to make an automated decision about the data subject. One application of this is credit rating an individual by computer, based on certain facts known about him or her. Automatic scoring for Housing allocation may be another. In such cases, the data subject is entitled to a description of the decision-making process. The description need not give away any trade secrets about particular techniques or software used to make these decisions.

The Act says that if any decision about a data subject is made by automatic means, the Council must inform the data subject that this is the case as soon as possible. The individual then has 21 days to demand that the Council reconsider its decision or review the decision based on any new information made available. The data subject can write to the Council to ensure that no decision is taken that significantly affects that individual based on automatic processing of personal information only. There are exemptions for automated decisions made when entering into a contract or carrying out a contract with data subjects, or under a statutory obligation where the decision is favourable to the data subject, but there must be a mechanism for the data subject to make representations.

Examples of the exemptions include the making of payments from bank autotellers and credit card companies authorising a higher credit limit. The Council must respond within 21 days confirming that no decisions are being taken. If decisions are being taken, then the data subject can request that the decision is reviewed and not taken by wholly automatic means.

### 2.5.6. Correction of Inaccurate Data

The data subject can ask a court to order correction, erasure or blocking of any false or factually misleading data. The data subject is entitled to claim compensation for any breach of the Act that has resulted in damage.

### 2.5.7. Compensation

An individual who suffers damage for any contravention of any requirement of the Act by the Council is entitled to seek compensation for damage though the courts. An individual who suffers distress is entitled to compensation if the individual also suffers damage or the contravention relates to the processing of personal data for the special purposes such as journalism, artistic or literary purposes. Where there is quantifiable financial damage, further damages for distress can be demanded. Where the data have been processed for use by the media, claims may be for distress alone.

### 2.5.8. Direct Marketing

An individual has the right to prevent processing for the purposes of direct marketing. Direct marketing is defined in the Act as meaning the communication by whatever means of any advertising or marketing material which is directed to particular individuals. The Council does not have to give the individual written notice that they have complied with the data subject notice. However, if the Council fails to comply, the individual can apply to the Courts for an order.

### 2.5.9. Data Accuracy

Data is inaccurate if it is incorrect or misleading in any matter of fact. The expression of opinions does not necessarily breach this Principle if they are accurately recorded. However, expressions of opinions ("I think this man is incompetent") are very different from hearsay comments on allegedly factual matters ("I think this man has been declared bankrupt"). To play safe, avoid any formal recording of opinions if they are likely to be contentious. There is not a problem if data is an accurate record of information obtained by the Council from the data subject or a third party and the Council has taken reasonable steps to ensure the accuracy of the data. Nor is there a problem if the data subject has notified the Council that the data is inaccurate and this fact is clearly indicated. It is not enough to say that, because the data was obtained from either the data subject or a third party, that the accuracy of the data was ensured at that time. In other words, the onus is on the Council to ensure that data it receives is indeed accurate.

Failure to keep data accurate and up to date could lead to an action by a data subject for compensation, or for amendment or erasure of the data. The significance of the inaccuracy, where the data came from, the steps taken to verify the data, the procedures for data entry, the procedures taken when the alleged inaccuracy came to light, the willingness to inform third parties to whom the inaccurate data had been passed of the correction, and other actions taken by the Council to mitigate the effects of the inaccuracy will all be taken into account. In short, the more reckless, slapdash or even indifferent you are to such allegations, the more likely you are to be sued successfully.

### 2.5.10. Archive and Backup Data

Backup and archived data are no longer exempt from subject information requests. This may have a significant cost implication for the Council where archived information is not easily or cheaply searchable to satisfy these requests.

### 2.5.11. Data Retention

The Act says that information must be kept only for as long as necessary. Therefore, be prepared to justify the retention period you have adopted. Data must be maintained for as long as is required for historical, legal, fiscal and auditing purposes (for example, for any Statute of Limitations to apply). Take legal advice on this matter. In the case of former employees, it is justifiable to maintain records for a period in case of queries on tax paid, or requests for references from third parties. Check if there are any Codes of Practice from professional bodies on these matters.

Records need only be kept up to date "where necessary". However, in most cases it will be considered as necessary. Exemptions will include for example, a static archive used for historical research, which need not be updated. Implement procedures for checking and updating data at regular intervals. The nature and frequency of these checks very much depends on the type of data collected and the purpose for which it is used. Whatever approach is taken, always adopt a pro- active approach for regular review of, and weeding out of old data.

## *2.6. Disclosure of Personal Information*

### 2.6.1. Corporate Induction

Council employees and agents must be trained on the new data protection regime. Corporate induction procedures should highlight the need for the correct working environment including:

- a clear desk practice
- secure telephone practice
- switch off/disable unattended workstations
- use of locks and passwords
- good office discipline and behaviour

They should also emphasis correct working practices such as:

- high levels of accuracy
- sharing information with authorised colleagues
- verifying external enquiries for personal information
- security of external/internal communications
- precautions against damage to information
- regular information “weeding” routines

As manual data is covered by the Act, employees should be told that they can not insert personal (and often inappropriate) remarks on paper files (e.g. "this customer can be difficult").

In the case of computerised information, the Council has already issued guidelines for good security practice in the 'IT Telecoms & User Security Policy'.

### 2.6.2. Departmental Induction

Departmental induction procedures will have to be reviewed to ensure that the Council's obligations under the Act are met. This includes the obligation to:

- have clear written information handling procedures in place

- ensure that employees are trained in the defined procedures
- ensure that employees are aware of their legal obligations

- ensure that employees are aware of the criminal penalties
- authorise the level of access to Council information systems

### 2.6.3. Processing personal data in accordance with instructions

Council employees and agents must abide by the provisions of the 1998 Act and only process personal data in accordance with management instructions. They must not deal with or generally use the personal data in any way outside their authorised duties.

### 2.6.4. Authorisation to process personal data

Management have an obligation under the Computer Misuse Act 1990 as well as the Data

Protection Act to clearly authorise the level of access to employees using Council systems so that criminal prosecutions may be brought in respect of any unauthorised access to data under the 1990 Act. Employees should be aware of what their authorisation is and should know not to exceed such authorisation.

### 2.6.5. Confidentiality

Council employees must not only abide by the duty of confidentiality they owe in respect of Council information, but also in respect of personal data. They must keep such personal data completely confidential, and must not disclose it unless authorised to do so. This duty must also be imposed on any third party processing personal information on the Council's behalf. Particular care must be taken when using the Council's e-mail system as electronic mail can never be assumed to be confidential unless appropriate technological measures are taken to make it so. As a general principle, personal information should not be transmitted by e-mail. See Section 2.8.5 for more information.

### 2.6.6. Security Measures

Employees must abide by the Council's specified security measures in respect of the personal data they process. This may be, for example, taking extra care when personal data are on a computer screen that no-one looks over the employee's shoulder, or if the employee takes work home on a lap top, that appropriate security measures are taken in respect of that laptop and its contents.

### 2.6.7. Disciplinary Procedures

Employees must be informed of the procedure for disciplinary proceedings in respect of a breach of the 1998 Act. They should know that in serious cases it would amount to gross misconduct leading to instant dismissal.

### 2.6.8. Criminal Liability

Employees should be aware that breach of the provisions of the 1998 Act might attract personal criminal liability. Criminal liability will arise if the employee, alone or with another, knowingly or recklessly obtains or discloses personal data without the employer's consent.

### 2.6.9. Manual Records

Over a period of time, manual files accumulate many items of information ranging from informal hand written notes, to extremely sensitive personal information such as health details, equal opportunities information, grievance procedures and other such forms. The Data Protection Act imposes a legal requirement to ensure that information held is adequate, relevant and not excessive for the purpose for which it is held. The information also needs to be accurate and up to date. This means that departments must have procedures in place to ensure that changes to personal information are correctly recorded in all files that reference the information.

#### 2.6.9.1. 'Weeding' of Personal Files

Departments must have policies and procedures in place to ensure that periodically, files are checked to ensure that redundant information, such as 'spent' disciplinary records, are removed. This may happen as part of normal access to the file, if all files are processed over a suitable period. Alternatively, it may be necessary to conduct a regular exercise to ensure that manual files meet the stringent data quality standards required by the Act. This exercise will also ensure that any informal and inappropriate comments made by staff members can be removed from the record to prevent embarrassment to the data subject or the Council should the information be released under the subject access provisions of the Act. Care should be taken to ensure that information that may be required for future legal or statutory purposes is retained in the file.

#### 2.6.9.2. Records Management and Storage

The legal requirement for data retention is highlighted in Section 2.3.5 (Fifth Principle Adherence). This applies equally to manual records as it does to automated information. This imposes a legal obligation on the Council to ensure that records moved from short term to long term archive storage are managed is such a way that:

- they can be efficiently retrieved in response to a subject access request
- they are kept for as long as required for legal and operational purposes, and that
- they are destroyed or archived following a well documented procedure.

Departments should have a written policy in place to ensure that this takes place.

#### 2.6.9.3. Destruction of Records

It is Council policy to destroy all Council material securely, either by using an office shredder or a confidential waste contractor to avoid any embarrassing mishaps, even if the material is not confidential.

### 2.6.10. Exemption for Crime and Taxation Purposes

Several exemptions apply for law enforcement and measures to administer taxation. The exemptions apply to personal data processed for the prevention and

detection of crime, the apprehension and prosecution of offenders and the assessment or collection of any tax or duty, or any imposition of a similar nature. The Office of the Information Commissioner has advised that, in their view, the council tax would be construed as falling within the exemptions contained in section 29 of the Act. Non-domestic rates would be treated in the same way as council tax.

The Act allows the Council withhold or disclose personal information or process it where not to do so would be likely to prejudice any particular crime or taxation function or to discharge its statutory functions. Information that involves assessing and applying risk classifications relating to taxation, or crime related to fraud involving public funds, is also exempt where it is used for the crime and taxation purposes.

The implication for the Council is that other organisations such as the utilities are permitted to disclose personal data on a case by case basis to the Council where not to do so would stand in the way of collection of tax. The exemption would also sanction the use of internal sources of data for council tax purposes. However, the exemption would not permit the disclosure of personal data held for council tax purposes on a reciprocal basis to outside organisations or to other departments within the Council for non-council tax purposes.

The Government has also embarked on a campaign that aims to eliminate benefit fraud. As part of this campaign called the National Fraud Initiative (NFI), information from one local authority, government department or agency is taken and compared with information from another to identify anomalies and inconsistencies. The basic premise underlying the fraud initiative is the belief that persons committing fraud are likely to target several organisations and that information should be shared to produce indicators of possible fraud for further investigation.

The main department involved in the NFI is the Department of Social Security (DSS) and its agencies. When requesting Housing or Council Tax Benefit information from a local authority the DSS is operating under powers granted to it under the Social Security Administration (Fraud) Act 1997. Other government departments such as the Inland Revenue and Customs and Excise may also approach local authorities with request for personal data for data matching purposes or fraud investigation.

The Audit Commission Act 1998 also provides an auditor with a right of access to every document relating to a body subject to audit which appears necessary to him for the purpose of his functions under the Act. More information is available in the Council's Data Matching Code of Practice.

### 2.6.11. Disclosure to Police Officers

The Act allows the Council to release personal information to the police for the prevention or detection of crime or the apprehension and prosecution of offenders if certain criteria are met. You are not obliged to disclose any data unless you have reasonable grounds for believing that any failure to do so would be likely to prejudice the purposes for which the data was requested. The Commissioner has also placed further interpretation on the Act, stating in her introduction to the 1998 Act that "there would have to be a substantial chance rather than a mere risk that in

a particular case the purposes would be noticeably damaged". What you need to obtain from the police are details of:

- The crime being investigated
- The reason for the enquiry (i.e. the appropriate DPA exemption purpose)
- How the absence of any information would be likely to prejudice the enquiry

Failure to meet these criteria could mean that the Council, the requesting officer or both are committing a criminal offence.

All police forces use a form called a section 29(3) form designed in association with the Commissioner and the Association of Chief Police Officers (ACPO). The form is only a request for information and a waiver of the Council's liability if personal information is disclosed. If the form is provided and you are satisfied the reason for the exemption is valid and happy to provide the information then you may do so if you wish.

To protect both the Council and the requesting officer from inadvertently breaching the Act, you should refuse this request if:

- the form has not been signed by both the requesting officer and an authorising officer and their full details given, or
- the authorising officer is not of a rank senior to that of the requesting officer, or
- the authorising officer is below the rank of Inspector.
-

The requesting and authorising officers should be aware that they are each making a statement that the conditions given are true, and that obtaining personal data under false pretences may be a criminal offence.

Ensure you keep copies of all section 29(3) forms as evidence in case the data subject challenges you regarding the disclosure. Also, note that the form may well contain information of a sensitive nature about a police suspect that must be stored appropriately and must not be disclosed further. If you still have reservations, and you do not wish to provide the data, then ask the police for a court order. You may come under pressure from the officers involved, as they may want to avoid the extra work involved in a court order. However, if you disclose information without satisfying yourself that the exemption is valid, you are in breach of the Data Protection Act.

### 2.6.12. Disclosure to Elected Members

The Council must comply with the principles of the Data Protection Act and operate within both the confines of the declared purpose for which the information was collected and the notification to the

Commissioner. Employees of the Council may disclose personal data to Elected Members where such disclosure is for the purpose declared and would not breach the Data Protection Principles. In order to

comply with this requirement, the Council will also have to ensure that it does not breach any duty of confidentiality under criminal or civil law. Clearly, there are situations where Elected Members would act as members of the Council, perhaps sitting on a committee undertaking Council business. In these circumstances, there would not be any issue on disclosure, provided this was consistent with the notification or the purpose that the information was collected.

Where Elected Members operating in some other capacity, perhaps as a representative of a constituency or for party political purposes request information, this disclosure would have to be justified by the purpose for which the personal information was collected.

The Act provides that personal data may always be disclosed at the request of or with the consent of the data subject. While the Council must be satisfied that the members are acting on behalf of and with the knowledge of the data subject, the Commissioner's advice is that the Council does not generally have to obtain the consent of the data subject to the disclosure of their data to a Councillor provided that the Elected Member represents the ward in which the data subject lives. In this case, there would be a reasonable presumption that the member is acting on behalf of the data subject. In other cases, or where the information is of a sensitive nature, it may be prudent to seek the signed consent of the data subject. In providing the information, the Council should make it clear that the information is provided for the purpose of the particular case only and must not be used for any other purpose. It would be good practice to note any requests for information from Elected Members.

Elected Members should note that where they hold personal data for constituency case work and they control the content and use of the data then they will need to fully comply with the Data Protection Act as well as notifying as a data controller in their own right. While the advice from the Information Commissioner states that written authority is not always required for Councillors to process personal information relating to constituents, consideration should be given to obtaining written authority from data subjects when processing personal information for the Councillor's own protection in case of any subsequent legal action.

Elected Members should also be aware that employees of the Council have a duty of care to ensure that personal information is only disclosed for the specified purposes under the Act. Therefore, requests for personal information should be made through the appropriate Head of Service to ensure compliance with Council procedures.

### 2.6.13. Disclosure to Utilities

Instances have arisen in the past where local authorities and public utilities have entered mutual agreements to exchange personal information for debt tracing purposes. The Commissioner has indicated that this practice is definitely unfair and likely to be unlawful breaching the First Principle of the Data Protection Act. Disclosure will only be justified where it would be in the substantial interest of the data subject or the substantial public interest. This will normally be in cases of emergency, but even here, disclosure would normally be to a representative of the police force rather than the utility company.

As discussed above under the exemptions for crime and taxation, other organisations such as the utilities are permitted to disclose personal data on a case by case basis to the Council where not to do so would stand in the way of collection of tax, including non-domestic rates. However, the exemption would not permit the disclosure of personal council tax data on a reciprocal basis to other Council departments or outside organisations, other than for council tax or non-domestic rates purposes.

### 2.6.14. Disclosure to Other Bodies

Where requests for personal information are received from other bodies such as the Inland Revenue, the Benefit Agency or the Child Support Agency, , it reasonable to expect that the request will be supported by a reference to the relevant legislation legitimising the disclosure of the personal information by the Council. If you are in any doubt about the legality of the disclosure, or no legal authority has been quoted then please consult the Legal section for advice. The Council will only be justified in disclosing personal information for debt tracing purposes on production of a court order or other satisfactory evidence that the information is required for the prevention of crime. This also applies to other agencies such as Sheriff Officers or other investigators who are pursuing debt. Remember that you may have to justify your decision in court.

### 2.6.15. Confidential References

It is customary to provide references for individuals regarding their suitability in particular circumstances related to education, training and employment, as well as for services they may provide. This kind of documentation can sometimes be the cause of considerable concern. The specific purposes of the references covered by the Act are identified and include:

- The education, training or employment, or prospective education, training or employment of the data subject.
- The appointment or prospective appointment of the data subject to any office.
- The provision or prospective provision by the data subject of any service.

The Act specifies that confidential references given by the Council about a data subject are exempt from the data access provisions so they remain confidential. Therefore, a writer of a reference in not obliged to provide the data subject with access to its contents while in the possession of the writer. However, the exemption covers confidential references given, or to be given. If it is intended to be confidential, the writer should clearly indicate on the material that it is being provided "in confidence".

The recipient of the reference does not get this exemption. People writing a reference should bear in mind that the data subject could have access to the reference once in the hands of the Council. The Council also has to take certain steps where the reference identifies a third party, for example, the writer of the reference. They would either have to seek permission from the writer, or de- personalise the reference.

Where it is not possible to secure permission from the writer, in extreme cases, the recipient will have to make a decision between the privacy interests of the writer and those of the data subject. In order to avoid this, the Council must move to a form of words on all requests stating that references are not given in confidence and giving consent to disclose the reference to the data subject.

### 2.6.16. Mortgage Applications and Other Loans

Section 2.7.14 relating to confidential references does not cover references given for other purposes such as mortgage applications or other loans. However, the information given is still personal information covered by the Data Protection Act. Appropriate steps will have to be taken to ensure that information disclosure only takes place with the written authority of the data subject; that the information given is accurate and up to date; and that appropriate security measures are in place to ensure that the information is disclosed to the correct party.

### 2.6.17. Electoral Registration

The Representation of the People Act (RPA) requires the Electoral Registration Officer (ERO) to make the register available for public inspection and to supply copies of the register to anyone who places an order. The ERO is allowed to do this, as there is specific exemption under the Data Protection Act 1998 for personal data held by a person under a duty to make them public. There is a further exemption where the person is required to make a disclosure of personal information by law.

The ERO has complete control over the collected data. The Council is not the data controller. He/she must ensure the data are ONLY used in accordance with the requirements of the RPA - i.e. made available for inspection and sold to those who order it. If the ERO exceeds these legal restrictions the data are no longer part of a "public document" and no longer used for the notified purpose.

There is clearly a case for the register to be available for inspection to ensure the transparency of the political process. There is also an argument that it should be available to political parties. However, with the developments in information technology, the register can now be used for a variety of purposes. The main use has been to compile credit reference files and for direct marketing. From 1 December 2001, when the RPA changes individuals will have the option to have their name excluded for direct marketing purposes. It will require two separate registers - a full one and one that excludes those people who opt out. Where the full register is made available to third parties, it will be under licence and there will be strict conditions excluding use for direct marketing purposes. While it is likely that the Council will be able to purchase the short version of the register, employees will have to ensure that they abide by the data protection principles and obey any licence conditions.

Any new purposes must be notified by the council (e.g. debt collection, person tracing, and fraud prevention) with the appropriate sources notified AND the data subjects must be made aware of these new purposes - positive consent may be required for some of these secondary purposes. In the interim, any complainants

can be advised that the Mailing Preference Service exists to help individuals reduce the amount of unsolicited mail that they receive.

### 2.6.18. Examination Results

- There is a special extension to the forty-day time limit if the personal data consists of marks or other information held to decide the results of examinations where the results have not yet been announced. In such situations, the Council must reply either within five months of the application, or within 40 days of the result being announced, the earlier of these two dates applying in all cases. The following points should be noted:
- This only applies to marks and not other information that may be in the same file (e.g. name and address). Normally this will relate to examination results within the Education service of the Council but can also refer to other examinations including psychometric testing for employment purposes.
- The data subject will have access to all the marks and other data held on file including any that they may not have seen previously.
- The five-month rule applies even although the results have still not been published.
- The normal rule that the reply may take into account routine amendments and deletions does not apply if the forty-day period is to be exceeded. In such cases, it will be necessary to ensure that all states in which the data have been held are recorded.
- If marks are unchecked or provisional, the applicant should be told this when the replies are sent out. The marks must still be sent out regardless of their current state.
- Note that the examination scripts themselves are explicitly excluded from subject access.

### 2.6.19. Release of Examination Results to the Media

Under the Education Act 1996, schools are required to provide information relating to pupils' examination results. This type of information does not identify individual pupils. The following advice applies to the publication of exam result information that identifies individual pupil's achievements. When considering a disclosure of personal information, you must ensure that any disclosure is justified under the Data Protection Principles. The First Principle is particularly relevant when disclosure of personal information is being considered. In order to be fair and lawful, the Council must ensure that data subjects are aware of any non-obvious uses or disclosures that may be made with their information at the time that they provide it and that the Council has properly notified the release of examination results to the press and media.

If a school has traditionally released results to the local press, and all pupils and their parents would be aware of this, then it is likely that this may be regarded as an 'obvious' disclosure. In these circumstances it would not, strictly speaking, be necessary to notify pupils that details of their results are to be passed on. However,

it would be good practice to do this so those new pupils to the school or the area are made aware that their results may be published and given the opportunity to object. If objections are received then these should be respected. Failure to do so would constitute "unfair processing".

If a school that has not previously passed results to the local press decides to do so then all pupils must be notified and given the opportunity to object. The results of those who do object should not be passed on. Similarly, pupils should be notified if any additional information is to be published, such as their intended universities or future employers. A notification can be included in any school publication or communication from the school to the parents but should occur before entry to the examination. The parents of younger children will make the decision on behalf of their children. Pupils themselves can be notified when the results relate to higher level examinations as they are therefore at an age when they can decide for themselves whether they wish to have their results withheld or not.

## *2.7. Information and Advice*

### 2.7.1. Third Party Processing

Under the Act, the Council has to notify and has a legal responsibility to ensure that ANY data relating to living individuals passed to a data processor is processed in compliance with the new Data Protection Act. A data processor is any person who processes the data on behalf of the Council other than an employee of the Council. That includes automated processing, manual records and accessible records (health, education, housing and social work records). Each department of the Council has a legal obligation to ensure that both new and existing contracts where personal information is passed to a third party must comply with the needs of the 1998 Act. Under the 1998 Act, the Council must have a written contract with the data processor to ensure the security of the data being processed.

Fairness in processing

Whichever condition is satisfied for processing personal data, the data controller must ensure that the processing is fair. This means that when obtaining data from a data subject, then you must ensure that the following information is made readily available:

- the identity of the Council
- the identity of any nominated representative for the purposes of the Act
- the purpose or purposes for which the data will be processed
- any other information necessary to ensure fairness: such as the likely consequences of the processing, and whether they envisage the data being disclosed to a third party.

In many cases where personal data are obtained from someone other than the data subject, the Council must provide the above information to the data subject. There are very limited exceptions from the fair processing code, but these do not absolve you from the overriding duty to process personal data fairly and lawfully.

The case for consent

So long as there is no likelihood of a significant adverse effect on the individual through processing their information, the specific consent of the data subject will not always be required. Where consent needs to be sought, the data subject should be left in no doubt that they are giving their consent - consent should be specific and informed. It cannot be inferred from non-response to a request or communication between a data controller and individual, nor can consent be deemed valid if given under duress or because of misleading information.

Even where consent has previously been given, then you cannot assume that this will endure forever, and individuals must be allowed to withdraw consent at anytime after it is provided. In many cases the data controller may not need to provide individuals with too much detail in order to ensure that he or she is informed (for example when providing address details for a newspaper delivery). In others, nothing less than clear written consent will be required. Here the individual will need to be assured that they are fully informed of the details of the purposes for which the information is being collected, the length of time it will be retained and any third parties to whom the information will be disclosed. When consent is being sought for processing sensitive data, explicit consent is required. This means that the individual is absolutely clear about the detail of the processing. This should include the type of data and information to be processed, the reasons for processing and any part of the processing which may have an effect on the individual (for example any parties to whom the data or information are disclosed).

### **2.7.2.** Secondary Use of Council Tax Data

Before using Council Tax information for other purposes, the Council will consider all the following questions. These questions also reflect the criteria that the ICO will use to decide whether to take action in response to a local authority's use of Council Tax information.

1. **Is it necessary for the local authority to use the information to carry out its statutory functions**? - Local authorities have a duty to provide a wide range of services to the public. In general, the rules of data protection will not prevent a local authority using the information it holds to administer the services it is required to provide. In normal circumstances, a local authority may only use or disclose Council Tax information for a purpose that falls outside the limits of its statutory responsibility if it seeks and obtains consent for this. An exception to this is where a failure to disclose personal information would be likely to prejudice a purpose such as crime prevention. We do not consider 'necessary' to mean a local authority cannot use Council Tax information to provide a service in a different way, or to provide a new service to the public. However, any use of Council Tax information must be a proportionate response to a particular issue. The following questions will help to assess this.
2. **If Council Tax information is used for another purpose, what effect will this have on the people the information is about?** - Information collected for Council Tax purposes contains key information such as a relatively complete and up-to-date list of local residents' names and addresses. It is difficult to see how a local authority's use of such information to carry out its statutory functions would be either unfair or detrimental. We take the view that individuals are likely to expect

their local authority to use the most current and complete information available to it to administer its services. Local authorities should be aware that some name and address information, for example, that relating to members of vulnerable groups, is particularly sensitive and should not be used or disclosed if to do so would put any individual at risk of harm.

3. **Would using the information cause unwarranted detriment to any individual?** - By 'detriment' we mean harm, damage or distress. Detriment could be caused where, for example, a local authority uses information about an eligible job applicant, that they once 'disregarded' for Council Tax payment purposes on the grounds of imprisonment, to prevent that person taking up employment with them. It is extremely important for a local authority to only use Council Tax information, and all the other personal information it holds, in a fair and responsible manner.

4. **Would using the information for another purpose benefit those the local authority provides services to?** - 'Benefit' can take a number of forms. It could mean, for example, providing services that are based on more efficient use of public money or that are easier for individuals to use. A good example of benefit would be using Council Tax information to set up a system that would stop individuals having to provide their contact details separately to all the various parts of the local authority.

5. **Is the information particularly sensitive?** - The sensitivity of information is not determined purely by its nature, but also by the context in which it is held. For example, the names and addresses of individuals can become sensitive if linked to their eligibility for asylum seekers' food vouchers. The names and addresses of certain members of the population can be particularly sensitive and this must be reflected in the protection they are given and what they are used for. Some information collected by local authorities for Council Tax purposes is in itself extremely sensitive, for example, that showing that someone is 'disregarded' for payment purposes on the grounds of imprisonment or detention under the Mental Health Act. Such information must not be used for any other purpose than assessing whether a person is 'disregarded'. Banking details provided so that a local authority can collect Council Tax payments may only be used for purposes directly connected to the administration of the Council Tax.

6. **Will the information be adequately protected from improper use or disclosure?** - Sharing Council Tax information within a local authority means that more people will have access to it and so there is a greater risk of it being misused or improperly disclosed. Any local authority wanting to make wider use of the information that it collects to administer Council Tax must put clear, authoritative rules in place to make sure the information remains adequately protected from misuse or improper disclosure. For example, it should be a disciplinary offence for employees with access to the information to abuse their access rights. The unlawful disclosure of personal information is a criminal offence under the Act.

7. **Is there an alternative to sharing information in a form that identifies individuals?** - In many cases, for example, where a local authority is planning its provision of future services, there will be no need to use information in a form that identifies people. For example, a local authority planning transport services for the elderly may need to know the numbers of people above a certain age living in a particular area. Its transport planners would not need to know who those people are. Wherever possible, privacy enhancing techniques such as the anonymisation

or aggregation of information should be used to prevent the unnecessary use or disclosure of personal information.

### 2.7.3. Internet & Email Policy and Procedures

As mentioned in the introduction, the definition of personal information in the Act means that Internet and e-mail messages are covered by the Act. This not only covers personal information in the body of e-mails, but also e-mail addresses as well. You should be aware that the Council has published Internet and Email policies and procedures that you must follow. Issues relating to the Data Protection Act are discussed below. Under the Act, personal data includes any information about a living identifiable individual, including their name, address, telephone number, email address and any other information about the individual. If you include such information in an email or attachment or collect such information on a web site then you are deemed to be 'processing' personal data and must abide by the law. In particular, you must not collect personal information without the individual concerned knowing that you are doing so and the purpose that you are going to use the information for. You will also have to ensure the information is accurate and up to date.

The individual also has the right to inspect what is held about them on the email system or in separate archives, as well as information collected on a web site. The individual can demand the correction of inaccurate information, the blocking or erasure of damaging information and can sue for damage caused by inaccurate information. The Act also imposes rules on storing of personal data. The data must only be kept for as long as it is needed for the purpose for which it was collected. Employees who store emails in personal folders or archives will have to ensure that personal information is not held for longer than is absolutely necessary and are stored in a way that allows easy identification, review and destruction if needed. Finally, the law imposes strict rules on the transfer of personal data outside the European Economic Area (EEA). Seek advice from the Council's data protection officer.

In order to avoid potential problems, it is important to realise that email is not a secure means of communication unless particular steps are taken to make it so. Personal information must only be included in messages when it is necessary to do so. Be aware that the data subject may inspect this information. Take care when you use distribution lists to send email messages to a group of people. It is possible to send the complete list of email users in the Council along with an external email. This could then leave the users vulnerable to 'junk' mail. Avoid this by ensuring that external emails sent to more than one recipient are sent using the 'Blind Carbon Copy' (BCC) option in your email software. You should be aware that all Internet access and email messages are logged and any inappropriate use will be investigated. This could lead to action under the Council's disciplinary procedure or legal penalties.

### 2.7.4. CCTV Policy and Procedures

The Council uses Closed Circuit Television (CCTV) cameras in two different areas. Firstly, in public places under the control of Thames Valley Police for crime prevention and secondly, under the control of individual departments for the protection of property against vandalism and theft. The Commissioner has

published guidelines that must be followed when CCTV cameras are installed and used. For the purposes of the Act, Thames Valley Police are data controllers for cameras in public places and are responsible for ensuring that operating procedures comply with the Act.

Any requests for subject access under the Act should be referred to them. Normally, contractors installing CCTV cameras will assist departments to ensure that they comply with all relevant legislation. However, it would be wise to review operating procedures to ensure that they are consistent across all council departments and that they comply with the Commissioner's Code of Practice. If you are responsible for a CCTV system then please contact the Council's Data Protection Officer to ensure that you are up to date with the latest information on the 1998 Act.

### 2.7.5. Geographical Information Systems

The use of Geographical Information Systems (GIS) in local authorities is a reflection of the growing awareness of the need for a different approach to the way that services are provided. The introduction of much new legislation and the pressure of 'Best Value' initiatives have lead to a change in the way that local authorities perceive their role and the services that they provide to the community. As well as continuing in its traditional role of providing a picture of the authority and its position in the wider geographic context, GIS is increasingly being used to determine the position of those most in need and the level of service required in each geographical area.

While GIS has traditionally been used by planning and development services within local authorities, Social Work, Education and Housing services are beginning to make use of GIS as a management and planning tool. Where services need to be put out to tender there is also a need to build up a profile of the service users. Such profiles need the ability to access different sources of information within the authority and bring them together to display on a map so that not only individual service users are being identified but also their location as well. The geographical information by itself is not a threat to the privacy of individuals.

However, developments in computer technology provide the facility to combine information initially gathered for different purposes for a new purpose and allow this information to be overlaid on maps. This use as a management tool where personal information is held as part of the system raises data protection issues. The data protection principles and data matching are fully discussed elsewhere in this document, together with the subject information requirements. Before combining geographical information with information from other sources, it is necessary to check for the existence of personal data that could be revealed. It is also necessary to ensure that there is no legal constraint on the use of data with GIS and that no breach of the data protection principles will occur. In summary:

- The use will be subject to the DPA if it contains information about living individuals.
- Ensure that the Council has a legal basis to use the data.
- Ensure that data subjects are aware of the purpose.

- Ensure that the purpose is included in the Council's DPA notification.
- Ensure that any new use is properly notified.
- If you need further advice then contact the Council's Data Protection Officer.

### 2.7.6. Sex Offenders Register and other Statutory Registers

The Council has a legal duty to participate in the maintenance of a Sex Offenders Register and other similar registers. This is a separate category of register and due care must be taken to ensure that detailed policies and procedures are established and that they comply with the appropriate legislation as well as the requirements of the DPA.

### 2.7.7. Crime and Disorder Act 1998

A common misconception appeared to exist regarding local authority information sharing under the Crime and Disorder Act. The Act does not allow indiscriminate information sharing or data matching between public authorities, including the police. Section 115 of the Crime and Disorder Act merely removes some legal obstacles to the sharing of data between these organisations. It does not automatically make that sharing lawful. Other legislation and the data protection principles still have to be followed.

The Commissioner has published guidance on the Crime and Disorder Act that gives more information. In summary, the Commissioner recommends that when setting up protocols or considering the use or disclosure of personal information, all of the following questions should be considered.

- What is the purpose of the information sharing agreement?
- Will it be necessary to share personal information in order to fulfil that purpose?
- Do the parties to the arrangement have the power to disclose personal information for that purpose?
- How much personal information will need to be shared in order to achieve the objectives of the arrangement?
- Should the consent of the individual be sought before disclosure is made?
- What if the consent of the individual is not sought, or is sought but withheld?
- How does the non-disclosure exemption apply?
- How do you ensure compliance with the other data protection principles?

By answering these questions, information sharing protocols will be developed and put in place so that there is a clear understanding between the partners as to what data may be disclosed and when, especially in the most common types of case.

## 2.8. Accessible Records

Accessible Records are records that were governed by previously existing statutory access rights e.g. medical records, social work records, housing records and education records accessible under the Access to Personal Files Act. Access to these files in now through the Data Protection Act 1998. Note that these records do not need to be structured reference files. They refer to ALL of the information held for the data subject regardless of whether it is contained in a structured file or not. Subject access must be complied with immediately but this requires a balanced approach as the subject access could open up access to third party information not directly relevant to the individual.

### 2.8.1. Education Records

This applies to any information which is processed by an education authority in Scotland for the purpose of the relevant function of the authority other than information processed by a teacher for the teacher's own use. An education authority, school and pupil are as defined in the Education (Scotland) Act 1980. In the case of a self-governing school, it is the board of management of the school. It covers previous and current pupils as well as individuals that receive or have received further education.

### 2.8.2. Social Work Records

This applies to information held for any purpose under the Council's past, present or future social work and education welfare functions. Provision is made for other bodies or voluntary organisations to be added to the list of bodies covered by these rules.

.

## 2.9. Notification

The Council is required to provide notification to the Office of the Commissioner of all processing undertaken by the Council as specified by the Data Protection Act and subordinate legislation. This process will be administered centrally by the Council's nominated Data Protection Officer who is the Head of IT Strategic Development. The Council's notification covers the majority of Council functions. However, other individuals or organisations associated with the Council who process personal information will be responsible for arranging their own notification. In particular, this requirement should be drawn to the attention of elected members, voluntary and urban funded projects, as well as services within the Council that have a separate legal status within the Council such as Assessors, Electoral Registration Officers and Registrars of Births, Deaths and Marriage.

The Notification must be renewed annually and any changes to the notification must be made within 28 days. Subordinate legislation imposes a duty on anyone who has a register entry to notify the Commissioner of any respect in which the entry becomes an inaccurate or incomplete statement of the current registration particulars or in which the latest description of security matters becomes inaccurate or incomplete. If the Council fails to do this then it is breaking the law. Departments must have procedures in place to ensure that any additional processing (or where processing has stopped) must be notified to the Data Protection Officer.

### 2.9.1. Exemptions

Subsidiary legislation to the Act provides exemption from notification for certain processing operations involving staff administration, advertising, marketing and public relations, accounts and record keeping and certain processing operations carried out by non-profit making organisations. These operations are considered unlikely to constitute processing harmful to the individual and will exempt some small businesses from the need to notify. However, the categories of processing listed in the previous paragraph must still comply with all of the Principles of the Data Protection Act. As the Council is still required to notify other areas of processing it will not take advantage of the exemption and will notify all processing.

### 2.9.2. Data Matching

Questions have been raised about the legal rights of Councils to get involved in data matching processes. The Commissioner's Office is concerned about the way in which local authorities are handling or proposing to handle Data Matching. Data Matching is primarily for the prevention and detection fraud. Many authorities are using information held on say, payroll files, to follow up non-payment of council tax for their employees. The Council will consult with the relevant unions and employees before proposing to implement Data Matching. For example, many banks have agreed the policy of data matching with their staff and unions and now have specific clauses included in all contracts of employment. The Council has drawn up a Code of Practice relating to Data Matching that will form the basis for any exercise conducted by the Council. The Government has also embarked on a campaign that aims to eliminate benefit fraud. As part of this campaign called the National Fraud Initiative (NFI), information from one local authority, government department or agency is taken and compared with information from another to identify anomalies and inconsistencies. Where such information disclosure is required by statute, the Council will endeavour to inform employees that the disclosure is taking place. Please see section 2.7.8 Exemption for Crime and Taxation Purposes for more information.

## *2.10. Enforcement*

It is the Council's intention to conduct its affairs in such a way that the powers listed in this section are never applied. However, they have been included for completeness and to illustrate that the Commissioner has significant powers of enforcement. Individuals have the power under the Act to complain to the Commissioner who can act on their behalf. The Commissioner has very greatly extended powers of enforcement under the 1998 Act.

An individual can request the Commissioner to make an assessment under section 42 as to whether personal data have been processed in accordance with the Act. To carry out the assessment, the Commissioner can serve an information notice under section 43 requiring the Council to provide specified information within a specified time. Failure to comply with an information notice is a criminal offence. If the Commissioner is satisfied that a data user is contravening the Act, an enforcement notice (under section 40) may be served requiring the Council to take specified action which may range from rectifying inaccurate data to stopping all processing. Failure to comply with an enforcement notice is a criminal offence. The

Council can appeal against an information notice or an enforcement notice but not a warrant for entry. An appeal suspends the operation of the notices.

### 2.10.1. Commissioner's Powers

If the Commissioner convinces a judge that the Council has contravened any of the data protection principles or committed any other offence under the Act and that evidence of either of these events may be found on any premises, the judge can grant a warrant to the Commissioner. The warrant has to be exercised within 7 days of the date of its issue and during the execution of the warrant; the Commissioner may search the premises and inspect, examine, operate and test any equipment and inspect and seize any documents or material.

The Commissioner has to give 7 days notice in writing to the occupier of premises demanding access to the premises and a judge may not issue a warrant unless access was unreasonably refused or, having granted access, the occupier unreasonably refused to comply with a request by the Commissioner to hand over any material. The occupier has to be notified by the Commissioner of the application for the warrant and must be given an opportunity of being heard by the judge unless the judge is satisfied that it is a matter of urgency or that compliance with notification to the occupier would defeat the object of the entry. Reasonable force may be used in execution of the warrant. The only defences are national security and any legal professional privilege in respect of matters arising out of the Data Protection Act. It is an offence to intentionally obstruct a person in the execution of a warrant or fail without reasonable excuse to assist.

## 3. Subject Information Procedure

1. The Data Protection Act provides data subjects with a right of access to personal data held about them and processed by the Council for its purposes irrespective of whether or not they are processed by manual or automated means. This section summarises the procedure to be followed by the officer nominated by the Council's Data Protection Officer to fulfil the subject information request.

2. In responding to such a request the Council is required to:
   (a) inform the data subject that it is processing information about that individual and to provide a description of the personal data of which the individual is the subject and details of the recipients or classes of recipients to whom the personal are disclosed.

   (b) provide the data subject with a copy of the information requested and any available information as to the sources of the data. This must be in intelligible form.

   (c) where decisions affecting the subject have been based solely on the automatic processing of data, to be provided with information as to the logic involved.

3. Such requests must be made in writing and accompanied by the access fee of £10. This fee can be waived if the applicant can provide proof (copy of a benefit

book or letter) of being in receipt of a means tested benefit. The request must also contain sufficient information to enable the authority to identify the person making the request and to locate the personal information sought. It is recognised that some individuals may have difficulty in making a written request: arrangements to facilitate obtaining access in such cases through an agent are described below.

4. The Council is not obliged to comply with subject information requests unless the conditions mentioned in item three above are satisfied. The period for response is 40 days commencing with the day on which these conditions are satisfied.

5. Where provision of the information requested involves issues of confidence or could result in serious harm to a third party individual; the authority need only provide that information which can be disclosed without breaching confidence or revealing the identity of the third party.

6. In order to enable the Council to deal promptly with requests for access to personal data, it will be necessary to establish procedures to assist both the data subjects and staff in processing the requests. Such procedures may involve the use of an access request form. These are not a requirement of the Data Protection Act and completion of them is purely voluntary and must not be regarded as compulsory for any one making a request. Their use, provided they supply the level of detail required, can be regarded as a written request.

7. Subject access procedures are necessary, as not all individuals will make a request in writing. Many may ask for information when calling at local offices; others, especially the home bound, during visits or through a third party; while some will use the telephone or e-mail. Any procedures adopted will have to be flexible to enable them to deal with the different approaches available to the public. You must not provide personal data in response to telephone requests. The requester should be asked for his/her name, address and telephone number (so that the authority has a record of the call); to put the request in writing and informed of any fee and that the Council does not provide personal data over the telephone. You should note that although couples may be held 'jointly and severally liable' for Council Tax and other benefits, this does not give each the right to access personal information relating to the other, without consent.

8. However, It is Council policy to be as open as possible. If you are satisfied about the identity of the individual and can answer a request made by the individual in person on the spot without any form filling or breaching any confidence then do so, as long as this is acceptable to the applicant. Point out the existence of the formal procedure but do not force people to use it if they just want the answer to a simple question. In the long run, appearing defensive or forcing people to use the formal approach will be counter-productive. Formal requests will either be sent directly to your establishment or forwarded to you from the Council's nominated data protection officer via the Head of Service. If you receive an application for a subject information request directly, then you must contact the Council's nominated data protection officer immediately to

ensure that all necessary steps are taken to collate any other information required to satisfy the subject information request.

9. The person concerned will probably know most of the information made available from the records already. Even so, it may be helpful if a member of staff is available to assist the individual in assimilating the material. You should consider whether to make available counselling, interpretation and support to enable individuals to understand fully and make positive use of the records relating to them. Particular care should be taken to provide skilled counselling where appropriate - preferably by someone known to and trusted by the individual - where there is any possibility of him or another person suffering serious harm as a result of information becoming available to him or her.

10. The following is a breakdown of the steps involved in dealing with a subject information request.

## STAGE ONE.

Receipt of request.

Requests for subject access are likely to be made by any of the following methods:

1. In writing or by e-mail
2. In person (visit to authority)
3. Via a third party - (a) member of staff (b) other
4. By telephone

All written requests (including forms completed by members of staff and e-mail requests), should be passed to Paul Wheeler who is the Council's Data Protection Officer. Staff receiving requests made in person should ask the applicant to complete an application form or to submit a written request.

## STAGE TWO.

Validating the request 1 - Written requests

Check request for identification details and information necessary to trace the personal data requested; check for receipt of fee. Record receipt of fee and acknowledge receipt of request asking for additional information required to enable the request to be processed and any fee if this did not accompany the written request. Record the request on the Corporate system (REACT)

2 & 3 - In person, via third party - Ask for confirmation of identity.

Ask for written confirmation of authority where a third party is acting for the data subject. In any event requests for subject access from third parties should be referred to a senior manager.

Provide an application form, explain that it is not compulsory and offer to assist in its completion. Staff acting on behalf of the individual are required to complete the application form which, where possible should be signed by that individual. Ask for any fee and record receipt.

4 - Telephone requests

Ask for enquirer's name, address & telephone number Ask for request in writing and any fee explaining that personal data cannot be provided by telephone.

## **STAGE THREE**.

Providing the Information requested

Check the information provided by the subject's written request or via the completed application form against the Council's IT and manual record systems to establish if personal data are held about that individual and processed for any of the Council's purposes. Having established that the authority holds information in respect of that individual, identify locations where the data could be held and examine the contents to:

- establish the sources of such data in order to identify third party individuals who could be at risk of severe harm if data revealing their identity were to be disclosed to the subject
- check data provided by third party sources for any indications as to confidentiality and the existence of permissions to disclose. Where possible such individuals should be contacted in order to obtain permission to disclose
- where the data about the subject contains information about his/her mental or physical health check with the appropriate health professional that there are no objections to disclosure of that data to the data subject
- check that the contents are not covered by any exemptions listed in Section 3.5.
- if the personal information contains information originating from or supplied by the Principal Reporter to the Children's Panel, then the Principal Reporter must be informed within fourteen days of the request being received. The information must not be communicated without the permission of the Principal Reporter.
- check the authority's records to establish when last the individual requested access and the frequency with which such requests are being made

When individuals make a subject information request they are entitled to be supplied with a copy of the data as held when the application was received or when the request was answered, provided that any updates which occur are due to normal practice. You are not allowed to amend or destroy any information before issuing a copy of the data if this action is because of the subject information request. Laundering of data before despatch is strictly prohibited. However, if a routine update occurs after receipt of the access request and the reply being processed, the new data can be sent. Applications should never be held back because an update is pending. If data is no longer available about the data subject because of a routine update then the data subject should be informed of this in writing.

Extract as much of the personal information requested as is possible following the above checks and ensuring that information about other individuals, whose names appear on the same file (e.g. a member of the subject's family), is not included unless the information was originally supplied by the data subject.

Provide the data subject with a copy of the personal information and details of the purposes for which it is held, and the recipients to whom such data may be disclosed and where possible information as to the sources of the data.

There is an exemption where a third party is legally acting on behalf of the data subject and the data subject does not wish the information disclosed. This would apply to information given by the data subject in the expectation that it would not be disclosed to the person making the request. It may also be obtained as a result of any examination or investigation to which the data subject consented in the expectation that that the information would not be disclosed. It also applies to information that the data subject has expressly indicated should not be disclosed. This may be because the data subject is a person under the age of sixteen and the person has legal responsibility for the data subject or the data subject is incapable of managing his own affairs and the person has been appointed by a court to manage those affairs.

Ensure that all of the data requested is provided within the 40 days allowed by the Data Protection Act. Where this is not possible as much of the information that can be should be provided within that period together with an explanation of why it is not possible to provide all of the data; provided, that is, that to do so would not result in serious harm to third party individuals or prejudice to the individual. Retain a record that the data have been provided to the subject and the date on which they were provided. This may be by proof of posting using recorded delivery or other means.

### 3.1. Identifying the individual

The Council will need to be satisfied as to the identity of the individual making the request. Where a person's identity is uncertain, the Council will inform the applicant of the additional information required to establish the identity of the applicant. The applicant will need to provide any information that the Council may reasonably require identifying the individual. Where the applicant doesn't provide adequate information, the Council will not comply with the access request.

The applicant should be informed of this in writing. If the personal information held is not considered very sensitive and the applicant specifically requests the reply to be sent to the applicant's known address, the usual signature of the person may be sufficient proof of identity. If unintentional disclosure of the information to a person other that the data subject would be likely to cause damage or distress, the Council may reasonably require further positive proof of identity and take any other steps to ensure that the information is delivered to the correct individual. Possible methods of checking identity in these cases include:

- asking the individual to give information which has been recorded as personal data by the Council and which the individual might be expected to know. For example, if the personal data are contained in a personnel record, it would be reasonable to ask the individual to supply his or her date of birth and National Insurance number

- asking the applicant to produce a document which could be expected to be in his or her possession - either a communication from the Council or an official document such as a driving licence or benefit book.
- asking the individual to have his or her signature witnessed by another person aged over 18 years who is not a relative. The witness could be required to provide his or her full name and current address and to certify that, to the best of his or her belief, the applicant is who he or she claims to be.

If there are genuine reasons for suspecting that an individual has improperly made a subject access request in the name of another individual, the matter should be referred to senior management and appropriate legal advice sought. The Council may consider reporting the matter to the police.

### 3.2. ights of children and their parents

The Act does not distinguish between children and adults. Requests from children for access to personal information should be treated in accordance with the existing law of Scotland and the legal capacity of each child. A parent or guardian can make a request under the Act on behalf of a child but this information can only be provided if it facilitates the proper performance of parental responsibilities. The parent must be able to show that it is in the interest of the child and, where appropriate, that it is with the informed consent and understanding of the child. While a child of twelve or over can be presumed to have sufficient age and maturity to understand and provide informed consent, a child under twelve may possess sufficient understanding and maturity to be considered when a decision is made about the release of information. Each case must be treated on its merits to balance the rights of the child and the parents or guardian. As the right being exercised is statutory and not contractual the consent of the parent or guardian to the child's request for access to information is not required.

In many cases where the Council holds personal information on young people under sixteen this information is normally disclosed to their parent or guardians. For this reason, the Council will also accept applications from parents of young people who are under sixteen years of age and where possible these will be answered. However, proper care should be given to the type of information passed on. Careful consideration must be given to preserve information supplied in confidence, while balancing the need for information by parents to fulfil their parental responsibilities.

No person, including a child's parent or guardian, may exercise the right of access to personal information about that child without the child's informed consent. It is for local authorities to satisfy themselves on this account. If a local authority complies with an unauthorised request, it might be liable to an action for compensation for breach of confidence. It must be stressed here that in answering requests by parents of young people under sixteen they are not being provided with subject access under the Act, but making a normal disclosure of information as allowed by the Council's notification under the Act or as required by other legislation. Parents of young people under sixteen have a legitimate interest in such information and it would not make sense to deny them access to it under the Act if it were agreed practice to show them the information under other circumstances. In the Council's

notification, relatives, guardians and other persons associated with the data subject are listed as recipients of personal information about the data subject.

Normal administrative information held in Council records will not normally create problems if disclosed to young people, their parents or guardians. However, do not accept applications from parents of young people who are sixteen or over as the person can apply on their own behalf. Of course, there will still be occasions when information is given in the normal course of events as allowed by the Council's notification.

There is an exemption where a third party is legally acting on behalf of the data subject and the data subject does not wish the information disclosed. This would apply to information given by the data subject in the expectation that it would not be disclosed to the person making the request. It may also be obtained as a result of any examination or investigation to which the data subject consented in the expectation that that the information would not be disclosed. It also applies to information that the data subject has expressly indicated should not be disclosed. This may be because the data subject is a person under the age of sixteen and the person has legal responsibility for the data subject or the data subject is incapable of managing his or her own affairs and the person has been appointed by a court to manage those affairs.

In some circumstances, there may be doubt as to whether a child has the mental capacity to make a request. In such instances, a local authority is required to recognise that the child's legal rights are the same as those of an adult. The ability to complete an application form or make out a written request that is coherent may be sufficient. Where a child has insufficient mental capacity to make a personal application, facilities exist to make a request through an agent. Parents and guardians may make a subject access request in respect of information held about themselves on the child's file. References to "parent"" and "guardian" above are intended to include any persons at the time of the request who had acquired an interest by process of law, and specifically includes adoptive parents and local authorities. Such terms do not include natural parents whose rights have been lost under any statutory provision. Extreme care should be taken to avoid subject information requests being used as a method by which estranged parents can trace children. There may be situations where access to simple information, e.g. the child's address, could cause serious harm to the child. Therefore, you should exercise caution to protect the child's interest. If any parent is unable to state the current address of a child who is the subject of an access request, the address should not be part of any reply.

Equally, data that could assist in the location of a child should be removed, for example the name of the school attended. As a first step the parent or guardian with whom the child is currently residing should be contacted to see if written permission for the disclosure would be given. If consent is not given, then a senior officer of the Council will contact the applicant to see if evidence of status can be provided and whether a copy of the data without addresses or other such indicators of location would be accepted. If no satisfactory solution can be reached then the appropriate senior officer of the Council will contact Legal Services for advice on how to proceed further.

### 3.3. Request through an Agent

Any competent adult or child may make a request for access through an agent. A local authority receiving such a request must respond where it is satisfied that the person has authorised the agent to make the application. It is the agent's responsibility to produce satisfactory evidence that he has such authority. This may consist of a written authority signed by the individual, either limited to this particular application or more generally, or a general power of attorney. It is also possible for a person to assume responsibility for the affairs of another (on a temporary or permanent basis) without any particular authority but who would reasonably expect to get that authority if they applied. In some cases, it may be necessary for the authority to seek legal advice as to whether the agent can be regarded as having been properly authorised to act in the individual's interest.

There is an exemption where a third party is legally acting on behalf of the data subject and the data subject does not wish the information disclosed. This would apply to information given by the data subject in the expectation that it would not be disclosed to the person making the request. It may also be obtained as a result of any examination or investigation to which the data subject consented in the expectation that that the information would not be disclosed. It also applies to information that the data subject has expressly indicated should not be disclosed. This may be because the data subject is a person under the age of sixteen and the person has legal responsibility for the data subject or the data subject is incapable of managing his own affairs and the person has been appointed by a court to manage those affairs.

Elected representatives, such as Councillors, Members of Parliament and Members of the Scottish Parliament, have no particular rights of access to information about others. They may, however, act as an agent in the same way as other interested persons provided, of course, that the local authority is satisfied as to their having been authorised to act on the individual's behalf.

### 3.4. People with Mental Disorders

No special provision is made in the Act about requests for access in respect of person with mental disorders. Many such people will be perfectly capable of seeking access on their own account. Others may need assistance and applications on their behalf be made in the appropriate circumstances by a parent or guardian appointed to act for them - or simply by a friend, relative, or other person acting in their interest. In cases where the subject is a child, the advice above applies.

It has to be acknowledged that people who are profoundly handicapped or suffering from chronic mental health problems may not be able to signify consent for an agent to seek access on their behalf. In such circumstances the Council will wish to satisfy itself that the agent is acting in the interest of the person and may be guided by the views of the mental health officer or of staff in other caring agencies who provide services and who know the individual concerned.

## 4. Subject Information Notices

### 4.1. Absolute Right to Prevent Processing

The data subject is entitled to submit a notice in writing at any time to prevent within a reasonable time any processing that is causing, or is likely to cause unwarranted and substantial damage or distress to either themselves or other named individuals. The Council must establish procedures to process these data subject notices and respond to the data subject within 21 days of receiving the notice. The response must contain a statement on how the Council has complied or intends to comply with the notice, or the reasons for regarding the notice as unjustified.

The data subject cannot exercise this right:

- if the data subject has given consent to the processing. This could be verbal, although it is best to record it.
- if the processing is necessary for the performance of or entering into a contract to which the data subject is a party.
- if the Council is legally obliged to do the processing
- if the processing is necessary to protect the vital interests of the data subject.

### 4.2. Absolute Right to Prevent Processing for Direct Marketing

An individual has the right to prevent processing for the purposes of direct marketing. Direct marketing is defined in the Act as meaning the communication by whatever means of any advertising or marketing material which is directed to particular individuals. The Council must establish procedures to process these data subject notices and respond to the data subject within 21 days of receiving the notice. The Council does not have to give the individual written notice of compliance with the data subject notice. However, the Council will reply with a statement on how the Council has complied or intends to comply with the notice, or the reasons for regarding the notice as unjustified. If the Council fails to comply, the individual can apply to the Courts for an order.

The Council's current registration includes a purpose covering host mailing, whereby the Council uses data held by the Council to distribute promotional material on behalf of a third party. This currently occurs through payslip inserts and advertising on the payslips. Case law will be required to clarify whether this kind of processing constitutes direct marketing or not as it is distributed to all employees, rather than targeted at particular individuals. However, it is unlikely to cause any harm or distress.

### 4.3. Statement of Processing

A Statement of Processing must be supplied within 21 days if a data controller is not required to notify processing to the Commissioner. The Council will notify all processing under the Act and will state this in any response to enquiries.

5. Glossary of Terms

## Data

Information processed by means of equipment operating automatically in response to instructions given for that purpose.

## Data Controller

Person who alone or jointly with other people determines the purpose for which and the manner in which any personal data are processed, or are to be processed.

## Data Processor

Any person other than an employee of the Council who processes the data on behalf of the Council.

## Data Subject

The individual who is the subject of the personal data

## Information Commissioner

The 1998 Act gave the registrar a new title known as the 'Data Protection Commissioner' with wider enforcement powers and the new duty of promoting good practice. The Freedom of Information Act 2000 then gave the Commissioner additional responsibilities under the Act and changed the title to 'Information Commissioner'.

## Direct Marketing

All activities which make it possible to offer goods or services or to transmit other messages to a segment of the population by post, telephone or other direct means aimed at informing or soliciting a response from the data subject as well as any service ancillary thereto.

## Personal Data

Any information relating to a natural living person who can be identified from data or other information held by the Council, including expressions of opinion and evidence of intentions towards individuals. Examples of data that relate to a living individual include application forms, sickness and disciplinary records, appraisals or family & medical records.

Sensitive personal data

Personal data consisting of information on e.g.

- racial or ethnic origin
- political opinions
- religion or other beliefs
- trade union status
- physical or mental health/condition
- his/her sexual life
- alleged offences/sentences

## Relevant Filing System

Any set of information relating to individuals that is not automatically processed but forms part of a filing system which must be structured and accessible according to specific criteria e.g. index cards, microfiches and similar collections from which personal data are capable of being readily extracted.

## Manual Records

The Directive states that manual files are "relevant filing systems which mean any set of

information relating to individuals to the extent that, although the information is not automatically processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".

## Accessible Records

Accessible Records covers records governed by previously existing statutory access rights e.g. medical records, social work records, housing records and education records.

These records do not need to be structured reference files. However the Data Principles do apply and Notification is required after 2001. Subject access must be complied with but this requires a balanced approach as the subject access could open access to third party information not directly relevant to the individual.

Assessable Records

This is a new category of processing to be subject to close oversight by the Commissioner. Such processing is to be delayed until the expiry of specific time limits or the service of notices by the Commissioner, if within such time limits. The Commissioner is required to notify the Council as to the extent to which assessable processing is or is not likely to comply with provisions of the Act. The types of data to which it applies will be specified in subordinate legislation. None have been specified at this time.

## Processing Data

Obtaining, recording, or holding the data or carrying out any operation or set of operations on the data including -

- organisation, adaptation or alteration of the data
- retrieval, consultation or use of the data
- disclosure of the data by transmission, dissemination or otherwise making available
- alignment, combination, blocking, erasure or destruction of the data

The Act introduces special rules on the processing of 'sensitive data'. Processing of such data will be permissible where it is 'necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the Council in connection with employment'. This is consistent with the Directive, which allows the processing of sensitive data 'in the field of employment law' in certain circumstances.

## Individual Consent

Consent may be required to process personal data that is not categorised as sensitive if no other justification recognised by the Act is available - Schedule 2 and 3 of the Act. There are exemptions for seeking consent.

Processing may take place without consent if it is necessary for the performance of a contract to which the data subject is a party - if a contract of employment is included, it should be open to employers to include terms in employees' contracts to enable the handling of personnel records without consent. Consent is not

required if processing without consent is necessary in order for the employer to comply with a legal obligation or to protect the "vital interests" of the employee.

It is unclear at this stage whether employees will be able to give a one-off consent to all processing for personnel purposes or whether they will have to give consent each time. If they have to give consent each time, then the employer will face the possibility of having constantly to seek consent whenever certain personnel records are updated. Individual Rights The Act contains a range of enhanced rights for data subjects including e.g. under Clause 7 of the Act; an individual is entitled to:

- be given access and be informed of personal data relating to the individual that is being processed
- be given a description of the data
- be given any information as to the source of the data
- know the purpose for which the data is being processed
- know the recipient/s whom they are or may be disclosed
- be informed of the logic behind any automated decision making
- to have communicated to him/her, in an intelligible form, the information constituting any personal data of which the individual is the subject and to have communicated any information available to the Council as to the source of those data
- the right to prevent processing of personal data where this may cause damage or distress
- the right to prevent processing of personal data for direct marketing purposes
- seek compensation/judicial remedy for damage caused by the Council's failure to comply with the requirements of the Act.

The individual right of access to personal data will continue. The forty day period for responding to a written request will commence on receipt of the fee of £10, and any information necessary to identify the individual. An individual will have the right to claim compensation where the Council contravenes certain requirements of the legislation. In the case of inaccurate data, an individual will be able to apply to the courts for correction, blocking, erasure or destruction. Not all information has to be disclosed. There are obvious exceptions for national security and public interest, but employment and educational references will not have to be disclosed and neither will information that cannot be disclosed without also disclosing information relating to another person. For example, this may be the name of the supplier of the information in a letter of complaint.

No automated employment decisions may be taken except where the decision relates to making a contract at the request of the individual or where his or her rights are protected. The protection will probably be a matter for a code or regulations. This provision will affect psychometric tests and Curriculum Vitae reading software on which decisions are solely based (it will not apply to decisions based on several inputs). Even if the test is permitted, the person will be entitled to know the general logic of the decision making which may be impractical.

Last updated October 2015
Version 4