Ysgol Dyffryn School

Data Protection Policy

Approved September 2017

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

DATA PROTECTION POLICY

1. Neath Port Talbot County Borough Council [hereinafter referred to as "the Authority"] is committed to ensuring its compliance with the requirements of the Data Protection Act 1998 ('the Act'). We recognise the importance of personal data to our organisation and the importance of respecting the privacy rights of individuals. This Data Protection Policy ('the Policy') sets out the principles which we will apply to our processing of personal data so that we not only safeguard one of our most valuable assets, but also process personal data in accordance with the law.

2. It is the responsibility of all our employees to assist the Authority to comply with this Policy. In order to help employees comply, we have produced a Data Protection Policy Guidance Note ('the Guidance') which explains in more detail the requirements of the Act. Employees must familiarise themselves with both this Policy and the Guidance and apply their provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal. Furthermore, serious breaches of the Data Protection Act could also result in personal criminal liability for the staff concerned.

3. In addition, a failure to comply with this Policy could expose the business to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data) or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

4. For these reasons, it is important that all employees familiarise themselves with this Policy and the Guidance.

Data protection principles

5. The Authority will comply with the following principles in respect of any personal data which it processes as a data controller:

5.1 Personal data must be processed fairly and lawfully and must not be processed unless:

5.1.1 at least one of the conditions in Schedule 2 to the Act is met; and

5.1.2 in the case of sensitive personal data, at least one of the conditions in Schedule 3 to the Act is also met.

The Schedule 2 and 3 conditions are set out in the Guidance.

5.2 Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes.

5.3 Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

5.4 Personal data must be accurate and, where necessary, kept up to date.

5.5 Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.

5.6 Personal data must be processed in accordance with the rights of data subjects under the Act. These rights are:-

5.6.1 the right of subject access;

5.6.2 the right to prevent processing likely to cause damage or distress;

5.6.3 the right to prevent processing for purposes of direct marketing; and

5.6.4 the right to object to automated decision-taking.

5.7 Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

5.8 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.9 This Policy may be amended from time to time to reflect any changes in legislation.

February 2008

Annex 2

DATA PROTECTION POLICY

GUIDANCE NOTE

1. INTRODUCTION

1.1 This Guidance Note ('the Guidance') forms part of the Data Protection Policy and provides supplementary information to enable employees to better understand and comply with the Data Protection Policy.

1.2.1 Neath Port Talbot County Borough Council [hereinafter referred to as "the Authority"] is required to comply with the Data Protection Act 1998 ('the Act') in respect of its processing of personal data (such as information about our customers, clients/service users, employees and contractors/suppliers). It is important for all employees to familiarise themselves with both the Data Protection Policy and this Guidance so that any processing of personal data can be carried out in accordance with the Act.

1.2.2 You should be aware that there is other legislation regulating public access to information such as the Freedom of Information Act 2000 which sometimes must be read in conjunction with the Data Protection Act 1998. There is further guidance on this on the Council's internet site.

1.3 You are required to assist the Authority to comply with its obligations under the Act. In order to do this you must comply with the Data Protection Policy and this Guidance whenever you process personal data, as well as any other data protection related policy that may be applicable to your area of work. ANY FAILURE TO COMPLY WITH THIS POLICY MAY BE A DISCIPLINARY OFFENCE WHICH COULD RESULT IN DISMISSAL. NEGLIGENT OR DELIBERATE BREACHES OF THE ACT COULD ALSO RESULT IN CRIMINAL LIABILITY FOR YOU PERSONALLY.

2. LEGAL FRAMEWORK

2.1 The Act sets out eight data protection principles which must be followed in relation to all processing of personal data. These principles are set out in the Data Protection Policy and are reproduced below, together with an explanation of what they require.

2.2 The Authority processes personal data about a wide range of data subjects, such as employees, clients/customers/service users, members, and suppliers/contractors. We process personal data for a number of purposes, such

as administration, marketing, profiling our clients/customers/service users. It is critical to our business that we are able to use personal data in this way. In order to continue to be able to do so, we must ensure compliance with the principles set out in the Act.

3. DEFINITIONS

3.1 In order to fully appreciate the requirements of the Act it is important for you to understand the meaning of certain key words and phrases which are used within the Act. These are set out below:

— **Data**—is information that is processed electronically; is manually (eg on paper); is recorded as part of a relevant filing system (see below); or is none of these but forms part of an accessible record; it can include non verbal data such as photographs

— **Data controller**—is the organisation that determines the purposes for which and the manner in which personal data are processed. The Authority is the data controller. Employees, managers, contractors and other staff are not data controllers;

— **Data processor**—is an external organisation that we appoint to process personal data on our behalf. Examples of these might include IT outsourced services providers *or* our external pensions provider;

— **Data subject**—is a living, identifiable individual about whom we process personal data;

— **Information Commissioner**—is the supervisory authority responsible for enforcing the provisions of the Act in England and Wales;

— **Personal data**—are data which relate to a living individual who can be identified from those data or from those data and other information which is in our possession or likely to come into our possession. Personal data include opinions and indications of our intentions towards an individual;

— **Processing**—has a wide meaning and covers virtually anything that can be done in relation to personal data, such as obtaining, recording, holding, altering, retrieving, consulting, using, disclosing, blocking, erasing or destroying personal data;

— **Relevant filing system**—is a set of manual information (ie paper files) relating to individuals which is structured by reference to individuals or criteria relating

to them in such a way that specific information relating to a particular individual is readily accessible;

— **Sensitive personal data**—means information as to (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) his trade union membership, (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, and (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

4. THE PRINCIPLES

4.1 First principle

4.1.1 Personal data must be processed fairly and lawfully and must not be processed unless (a) at least one of the conditions in Schedule 2 is met and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

4.1.2 This is the first and possibly most important of all the principles. It requires us to process personal data fairly and lawfully. Each of these requirements is considered in turn below.

Lawful processing

4.1.3 The Act prohibits the processing of any personal data unless that processing can be justified under one of a number of conditions which are set out in Schedules 2 and 3 of the Act. It is worth remembering the very broad definition of 'processing' which includes obtaining, disclosing, using and viewing.

4.1.4 You must justify your processing of **all** personal data under one of the conditions set out in Schedule 2. If you cannot find a condition that justifies your processing then that processing may **not** take place.

4.1.5 Schedule 2 conditions

1 The data subject has given his consent to the processing.

2 The processing is necessary in order to enter into or perform a contract with the data subject.

3 The processing is necessary for compliance with any legal obligation to which the Authority is subject (other than an obligation imposed by contract).

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary for the (a) administration of justice, (b) exercise of any functions conferred on any person by or under any enactment, (c) exercise of any functions of the Crown, a Minister of the Crown or a government department, or (d) exercise of any other functions of a public nature exercised in the public interest by any person.

6 The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, 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.

4.1.6 When considering the above conditions remember the broad definition of processing. For example, obtaining consent to processing means obtaining consent to the disclosure, collection, use, destruction etc of personal data.

4.1.7 In addition, where you are processing sensitive personal data, you must also justify that processing under one of the conditions in Schedule 3. This is a safeguard which recognises the sensitive and sometimes confidential nature of this category of personal data. The most relevant Schedule 3 conditions are set out below.

4.1.8 Schedule 3 conditions

1 The data subject has given his explicit consent to the processing.

2 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the Authority in connection with employment.

3 The processing is necessary (a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing (a) is necessary for the purposes of, or in connection with, any actual or prospective legal proceedings, (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

5 The processing is necessary for the (a) administration of justice, (b) exercise of any functions conferred on any person by or under any enactment, or (c) exercise of any functions of the Crown, a Minister of the Crown or a government department.

6 The processing is necessary for medical purposes and is undertaken by (a) a health professional or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

7 The processing (a) is of sensitive personal data consisting of information as to racial or ethnic origin, (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

8 The processing (a) is in the substantial public interest, (b) is necessary for the purposes of the prevention or detection of any unlawful act, and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

9 The processing (a) is of sensitive personal data consisting of information as to religious beliefs or other beliefs of a similar nature; or physical or mental health or condition, (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons holding different religious beliefs; or different states of physical or mental health or conditions, with a view to enabling such equality to be promoted or maintained, and (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

10 The processing (a) is in the substantial public interest, (b) is necessary for research purposes, (c) does not support measures or decisions with respect

to any particular data subject otherwise than with the explicit consent of that data subject, and (d) does not cause, nor is likely to cause, substantial damage or distress to the data subject or any other person.

4.1.9 Remember: unless you can justify your processing of sensitive personal data under both Schedules 2 and 3, you may **not** process those data.

Fair processing

4.1.10 The second requirement of the first principle is that personal data must be processed fairly. In broad terms what this means is that we must ensure transparency of processing so that data subjects are aware of who is processing their personal data and why. We achieve this by giving data subjects a Fair Processing Notice which meets the following requirements:

4.1.11 Content of Fair Processing Notice:

which shall contain

the identity of the data controller (ie the Authority),

the purposes for the processing ,

any other information that is necessary to make the processing fair (such as any recipients of the data and their purposes, a reminder of the data subject's right of access and correction and whether any of the information we are asking for is mandatory or voluntary) and

the notice should as far as practicable be written in plain language and not be unnecessarily complicated.

4.1.12 Timing of Fair Processing Notice:

4.1.12.1 The notice must be given to the data subject at the right time. Where we obtain personal data directly from the data subject (eg as a result of a telephone call, or online journey) we must give the notice to the data subject at the time we obtain his data

4.1.12.2 Where we obtain personal data about a data subject from a third party source (eg a family member) we must provide the notice as soon as reasonably practicable after we have started processing his data (unless it would be a disproportionate effort to do so)

4.1.13 Position and format of Fair Processing Notice:

The Fair Processing Notice must be reasonably prominent and in a reasonably legible font

The notice must be included at every point where we collect personal data, such as application forms or websites

If, for example, the notice is provided online, it must be positioned so that it can be seen and not hidden behind a hypertext link

4.2 Second principle

4.2.1 Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes.

4.2.2 The second data protection principle sets out two requirements:

— personal data must be obtained only for one or more specified and lawful purposes. Our Fair Processing Notices will specify the purposes for which we will process personal data and we are not permitted to process those data for a new purpose (unless the data subject gives his consent).

— personal data must not be further processed in any manner incompatible with the purpose or purposes for which the data were obtained. A breach of this principle could also result in a breach of the first principle. For example, if a Fair Processing Notice describes the purposes for which personal data will be used as administration and risk assessment, we should not use those data for any other purposes, unless those additional purposes would be totally obvious to the individual. To do otherwise could result in unfair processing in breach of the first principle and a breach of the second principle.

4.3 Third principle

4.3.1 Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4.3.2 The third data protection principle requires that personal data must be adequate, relevant and not excessive. You must, therefore, ensure:

— you identify the personal data needed for a particular purpose and you collect the minimum amount required to properly fulfil that purpose

— you do not hold personal data on a ‘just-in-case’ basis because you think it might be useful in the future but without having any clear idea of what that future purpose might be

— you keep data up to date (or else data which were originally adequate may cease to be so)

— you do not keep data for too long (otherwise those data may cease to be relevant and its retention may be an excessive holding of information).

4.4 Fourth principle

4.4.1 Personal data must be accurate and, where necessary, kept up to date.

4.4.2 Personal data will be inaccurate if they are incorrect or misleading as to any matter of fact (eg an incorrect name or address). If you are inputting data onto our system and are unsure as to the accuracy of certain information (eg because you cannot read the handwriting or because it looks like an obvious mistake or omission), you should try to get in touch with the data subject to clarify the issue.

4.4.3 We will not be in breach of this principle, even if we are holding inaccurate data if:

— we accurately recorded those data when we received them from the data subject or a third party and

— we took reasonable steps to ensure the accuracy of those data and

— if the data subject has notified us that the data are inaccurate, we have taken steps to indicate this fact (eg by making a note that we have received an objection).

4.4.4 You must take reasonable steps to keep data up to date to the extent necessary. The purpose for which data are held will determine whether they need to be kept up to date or not. For example, historical records of transactions should not, as a general rule, be updated.

4.5 Fifth principle

4.5.1 Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.

4.5.2 You should review the personal data which you hold on a regular basis and delete any data which are no longer required in connection with the purpose for which they were originally obtained. When carrying out this exercise you should consider any legal or other requirements to retain data (including the Authority's Records Management Policy and its records retention and disposal schedules). You should also consider the type of relationship which the Authority has with the data subject and whether there is an expectation that we will retain data for any given period of time.

4.6 Sixth principle

4.6.1 Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

4.6.2 The rights which are referred to in the sixth principle are the data subject's rights in relation to:

— access to his or her personal data

— preventing processing likely to cause damage or distress

— preventing processing for the purposes of direct marketing

— automated decision-taking

4.6.3 If you receive a request in writing from an individual mentioning any of the above rights, you must pass that request promptly to your line manager for his/her attention as there are strict timescales within which we must respond.

4.7 Seventh principle

4.7.1 Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

4.7.2 The seventh principle requires the Authority to take technical and organisational measures to protect personal data which we process:

— technical measures include: software controls to restrict user access; up-to-date virus checking software; audit trail software; and encryption—all of which we have in place and manage through our IT department;

— organisational measures include: restricting access to buildings and computer rooms; ensuring secure disposal of information; and training staff on the care and handling of personal data—all of which you are responsible for complying with and applying to your daily routine.

4.7.3 The Act imposes upon the Authority additional obligations if we use third parties to process personal data on our behalf. Examples of these third parties might include external IT or pension providers.

4.7.4 Therefore, if you are responsible for the selection or appointment of any data processors, or are involved in contract negotiations with data processors:-

4.7.4.1 you must make sure that you only select data processors that provide sufficient guarantees in respect of the technical and organisational security measures they will use in relation to the processing of personal data;

4.7.4.2 you must enter into a contract in writing with each data processor. It is important to do this before the processing actually begins;

4.7.4.3 you must ensure that each processing contract makes it clear that data processors must only act on instructions from the Authority. We are responsible for the processing of all personal data, even if it is carried out on our behalf by a data processor. We must, therefore, maintain control over such processing at all times;

4.7.4.4 you must ensure that each data processor agrees to take appropriate technical and organisational measures to protect any personal data that it processes on our behalf from unauthorised or unlawful processing, accidental loss, destruction or damage. It is important that we specify any measures that must be taken;

4.7.4.5 you must ensure that we have the right to check the data processor's compliance with the terms of any processing contract. This may involve auditing the data processor from time to time to make sure that it is processing in accordance with our instructions and the security measures we have specified, as well as any other data protection related requirement of the Act;

4.7.4.6 if the data processor will be holding personal data on our behalf and we do not also have a copy of those data, we must make sure the processing contract includes a provision that requires the processor to assist us promptly with any

"subject access request" we might receive in relation to any of the data held by the data processor;

N.B. – A "subject access request" is a request received from a data subject asking for access to personal data which we process about him or her

4.7.4.7 you must ensure that upon termination of the processing contract, the processor promptly returns or destroys the personal data as directed by us;

4.7.4.8 if the data processor will be collecting personal data on our behalf, the processing contract must include an obligation upon the processor to give our Fair Processing Notice (which the processor is not allowed to modify) to all individuals about whom the processor collects personal data;

4.7.4.9 if the data processor proposes to use sub-processors to assist with the processing services, you should seek advice from the Authority's Data Protection Officer as this will have consequences for the Authority and specific provisions will need to be included in the processor agreement;

4.7.4.10 it is important to remember that just because we delegate some of our processing activities to a data processor does not mean that we can delegate our responsibility to comply with the Act.

4.8 Eighth principle

4.8.1 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4.8.2 You must not transfer any personal data to any country outside the European Economic Area ('EEA'), unless you are authorised to do so. The EEA comprises the EU Member States plus Iceland, Norway and Liechtenstein.

4.8.3 If you need to transfer personal data to a country outside the EEA you must consult with the Authority's Data Protection Officer who will advise you further on how to comply with the adequacy requirements of the eighth principle.

4.9 DATA SUBJECT RIGHTS

4.9.1 The sixth data protection principle requires us to comply with the rights of data subjects. It is important for you to familiarise yourself with these rights so

that you may be able to identify them more easily. Each one is described below.

Right of subject access

4.9.2 Data subjects have a right of access to their personal data. A request for access will usually include a request for specific or general information relating to the applicant. If we receive such a request we must provide a description of:

— the personal data relating to that data subject

— the purposes for which the data are being processed

— the recipients of the data

— the information constituting the personal data

— the source of those data (if available).

4.9.3 The Act lays down timescales within which we must comply with a request and requirements regarding how the information must be supplied. If you are authorised to handle subject access requests, you should follow the rules and procedures set out in the Guidance for Handling Subject Access Request in the Schedule to this Policy. If you are not authorised to handle such requests, you should not attempt to do so, but should forward the request to your line manager for his/her attention.

Right to prevent processing likely to cause damage or distress

4.9.4 Data subjects have the right to ask us not to process their personal data if:

— the processing of those data in a particular way or for a particular purpose is causing, or is likely to cause, substantial damage or substantial distress to that data subject or another person; and

— that damage or distress is, or would be, unwarranted.

4.9.5 You can usually identify a request to exercise this right because it will ask us to stop processing personal information about the individual. The Act lays down timescales within which we must comply with such a request. If you receive a request to stop processing you must forward it promptly to your line manager for his/her attention. You should not attempt to deal with a request on your own.

Right to prevent processing for the purposes of direct marketing

4.9.6 Data subjects have the right to request that we stop processing their personal data for direct marketing purposes. This means we must stop sending direct marketing materials to anyone that objects.

4.9.7 If you receive a request to exercise this right you should forward it promptly to your line manager for his/her attention who will take the appropriate action to ensure that the individual's details are suppressed on our marketing database and he or she is no longer contacted by us for marketing purposes.

Right to object to automated decision taking

4.9.8 Data subjects have the right to object to automated decisions being taken about them in relation to important matters that significantly affect them (such as evaluating performance at work, creditworthiness, reliability or conduct). This right is complex and subject to certain conditions. You can identify a request made under this right because it is likely to mention automated decisions or decisions made by computer and may ask us to take that decision again manually (ie using an individual instead of a computer).

4.9.9 If you receive a request from any person exercising their right to object to automated decisions being taken about them, you should forward that request promptly to your line manager for his/her attention. You should not try to handle the request yourself.

Additional data subject rights

4.9.10 In addition to the rights specifically referred to in the sixth principle, data subjects also have the following rights:

— the right to ask the Information Commissioner to carry out an assessment as to whether or not we are processing is in accordance with the Act. This means the data subject has the right to make a complaint to the Commissioner and ask him to investigate. The Commissioner is obliged to consider all such requests and this could result in an investigation of our processing activities;

— the right to take legal action against us in the courts and claim compensation for any damage (or damage and distress) the data subject has suffered as a result of a breach of the Act; and

— the right to apply to court for an order to rectify, block, erase or destroy inaccurate personal data and any expression of opinion based on those inaccurate data.

Consequences of non-compliance

4.10.1 If we are found to be in breach of the Act, the Information Commissioner may issue enforcement proceedings against us which could result in our being prevented from further using personal data, or be required to change our processing procedures, or have other conditions imposed upon us in respect of the processing of personal data. Enforcement action will usually have a cost and time implication for the business. However, more damaging might be any restrictions imposed upon us which prevent us from exploiting our databases. Additionally, the associated publicity could make us appear as an organisation that does not respect the privacy rights of individuals.

4.10.2 Affected data subjects may also take legal action against us and claim compensation for any breaches of the Act on our part that have resulted in damage (or damage and distress) to the data subject.

4.10.3 In certain circumstances, a negligent or deliberate breach of the Act could result in criminal liability not just for the Authority but for our employees also. For these reasons it is essential to comply with the provisions of the Data Protection Policy and this Guidance.

Contacts and responsibilities

4.11 If you have any queries regarding the Data Protection Policy, this Guidance or compliance with the Act in general, please contact the Authority's Data Protection Officer for further advice.

The Data Protection Policy and this Guidance will be updated from time to time by the Data Protection Officer to reflect any changes in legislation or in our methods or practices.
February 2008

SCHEDULE

GUIDANCE FOR HANDLING SUBJECT ACCESS REQUESTS

INTRODUCTION

Under the Data Protection Act 1998 ('Act'), individuals such as employees, customers and business contacts (collectively 'data subjects') have a general right of access to personal data which the Authority processes about them.

This Guidance is aimed at those members of staff who are authorised to handle access requests. If you are not one of these authorised members of staff, you should refer any request you receive to your Section Manager.

ANY FAILURE TO COMPLY WITH THIS GUIDANCE MAY BE A DISCIPLINARY OFFENCE WHICH COULD RESULT IN SUMMARY DISMISSAL. NEGLIGENT OR DELIBERATE BREACHES COULD RESULT IN CRIMINAL LIABILITY FOR YOU PERSONALLY.

HANDLING SUBJECT ACCESS REQUESTS

1 Identifying a request

A request for access (referred to as a '**subject access request**') is a request from a data subject to be given access to personal data which we process about him or her. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a subject access request even though it does not expressly refer to personal data or to the Data Protection Act 1998.

All requests for access should be immediately directed to your Section Manager. There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the Information Commissioner and/or legal action by the affected individual.

2 Requirements for a valid request

For a subject access request to be valid, it must satisfy the following requirements:

2.1 the request must be in **writing**. If a data subject makes a request by telephone or in person, he or she should be asked to put that request in writing.

2.2 the request must be accompanied by the appropriate **fee**. We can currently charge up to £10 for processing a request.

2.3 we must be able to **identify the data subject** making the request and then verify that identity. Typically we will request a copy of the data subject's driving licence or passport to enable us to establish his or her identity and signature (which should be compared to the signature on the Subject Access Request). We also ask for a recent utility bill (or equivalent) to verify the data subject's identity and address.

2.4 we must be able to **identify the information** being requested. For example, a subject access request may be made by someone who is both an employee and a customer. We can ask him or her to specify whether he or she is seeking access to his or her human resources file, customer records or both.

If the data subject makes a request that does not satisfy the above requirements you should write to him or her.

Unless the above requirements are met, we are not obliged to comply with a subject access request. However, we are obliged to notify the individual promptly if the fee is missing or if we require any information in order to fulfil the request.

3 Time period for satisfying a request

Once a valid subject access request is received, we have **40 days** in which to respond. This 40-day period does not start to run until all these requirements have been satisfied. You should make a note of when this period commences.

4 Information to be provided in response to a request

The data subject is entitled to receive a description of the following:

— the personal data we process about him or her;

— the purposes for which we process the data;

— the recipients to whom we may disclose the data;

— the information constituting his or her personal data;

— any information available regarding the source of the data;

— the logic behind any automated decision we have taken about him or her (see below).

The above information must be provided in an **intelligible form** and any technical terms, abbreviations or codes must be explained to him or her.

Information about the logic behind automated decisions

If we are specifically asked in a subject access request for information about the logic behind any automated decision that we have taken in relation to important matters relating to the data subject (eg his or her performance at work, his or her creditworthiness, his or her reliability or conduct), we must provide a description of the logic involved in that automated decision, subject to the following conditions:

4.1 the automated decision must have constituted the **sole** basis for the decision. For example, an application for credit which is conducted without any human intervention, other than to complete the application form, could be a decision which is taken solely by automatic means. However, if there is any element of human discretion as to whether or not to grant the credit, the decision would cease to be wholly automated and the data subject would not be entitled to a description of the logic.

4.2 in providing a description of the logic we are not required to reveal any information which constitutes a trade secret (eg the algorithm behind a credit scoring system).

5 How to locate information

The personal data we need to provide in response to a subject access request may be located in several of our electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, you may need to search all or some of the following:

5.1 electronic systems (eg databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV);

5.2 manual filing systems (eg human resources filing system);

5.3 data systems held externally by our data processors (eg external payroll service providers);

5.4 occupational health records held by the Occupational Health Department.

You should search these systems using the data subject's name, employee number, customer account number or other personal identifier as a search determinant.

6 Information to be supplied in response to a request

Once you have carried out the search and gathered the results, you will need to select the information to be supplied in response to the subject access request. The data subject is only entitled to receive information which constitutes his or her personal data.

The type of information that will be classified as personal data is any information which:

6.1 identifies the data subject (either directly from the data or from those data and other information which is in our possession or likely to come into our possession);

6.2 is biographical in a significant sense (eg it is more than a recording of the data subject's involvement in a matter or event that has no personal connotations, such as his or her attendance at a business meeting where his or her name appears in the list of attendees);

6.3 has the data subject as its focus (eg the information relates to the data subject personally rather than to some other person with whom he or she may have been involved or some transaction or event in which he or she may have figured);

6.4 affects the data subject's privacy, whether in his or her personal, or family life, business or professional capacity;

6.5 is an expression of opinion about the data subject;

6.6 is an indication of the intentions of the Authority or any other person towards the data subject (eg promotion prospects or redundancies).

Information about companies or other legal entities is not personal data. However, information about sole traders or partnerships will be, as the individuals within them are data subjects. Personal data relating to deceased persons are not covered by the Data Protection Act.

The right of access is subject to a number of conditions and exemptions, particularly where the personal data reveal information about another individual—these are covered in paragraphs 7 and 10 below.

Examples of information likely to constitute personal data:

— marketing lists containing a name together with contact details (eg address, telephone number, email);

— customer profile information;

— Human Resources information (eg salary details, appraisals);

— financial information (eg information about the data subject's tax liabilities, income, expenditure);

— medical information (eg medical history or condition, including pregnancy);

— images caught on CCTV camera

Examples of information that are unlikely to constitute personal data:

— the reference to the data subject's name in a document that contains no other personal data about that data subject (eg the inclusion of the data subject's name in a list of attendees in the minutes of a meeting where the individual simply attended in his or her official capacity);

— where the data subject's name appears in an email that has been sent to or copied to him or her, but where the content is not about him or her (eg emails sent to the data subject about the Authority's business dealings);

— information about the performance of a department or office.

7 Disclosing personal data relating to other individuals

This paragraph sets out what you should do when the data subject's personal data includes information that identifies another person (eg as a source or recipient of the data subject's personal data).

You should first consider whether the other person's information constitutes personal data relating to the data subject. If this is not the case, then we are not obliged to provide that information. The other person's data should be blanked out so that he or she is not identified.

Where the other person's information does form part of the data subject's personal data, then you should consider:

— whether the other person has consented to the disclosure of his or her information, or

— whether it is reasonable in all the circumstances to comply with the request without the consent of the other person (eg because consent has been withheld

or cannot be obtained, or because asking for consent might reveal the identity of the data subject).

In order to determine whether it is reasonable in all the circumstances to grant access, you should consider the following:

— any duty of confidentiality that we owe to the other person;

— any steps we have taken to obtain the consent of the other individual;

— whether the other individual is capable of giving consent; and

— any express refusal of consent by the other individual.

The following additional factors should also be considered:

— whether the other person is a recipient or one of a class of recipients who might act on the data to the data subject's disadvantage;
— whether the other person is the source of the information;
— whether the information is generally known by the data subject; and
— whether the data subject has a legitimate interest in the disclosure of the other person's information which he or she has made known to us.

Ultimately, whether or not it is reasonable to disclose the other person's information will depend upon all the circumstances and each request must be considered on a case-by-case basis.

If the decision is taken to withhold the other personal information, we still have an obligation to provide as much of the information requested as we can without disclosing the identity of the other person. This can usually be achieved by redacting the data (eg blanking out names or other identifying particulars). Always keep a record of what you have decided to do and your reasons for doing it.

8 How should the information be provided

The data subject is entitled to be provided with a copy of his or her personal data in a **permanent form** unless this is not possible, or would involve a disproportionate effort, or the data subject agrees otherwise.

In determining whether the provision of the data in permanent form is a disproportionate effort you should consider the following:

— the cost of providing the information;

— the time it will take to do so;

— how difficult it may be for us to provide it;

— the resources available within the organisation compared to the effort required.

These factors have to be balanced against the significance of the information to the data subject and any negative effect it will have on him or her if we do not provide it in permanent form.

If we cannot provide the data in permanent form, we must consider alternative ways of enabling the data subject to have access to the data. For example, we could invite him or her to our offices and allow him or her to view his or her data on screen, perhaps taking copies of the data that are of most interest to him or her (if this is possible). If we allow the data subject to view his or her data on our premises, we need to ensure he or she is supervised and does not have access to confidential information or the personal data of others.

In all other cases, we should aim to provide the information in hard-copy form, redacted where appropriate.

9 Requests made by third parties on behalf of the data subject

Occasionally we may receive a request for subject access by a third party (an 'agent') acting on behalf of a data subject. These agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that he or she is authorised to act on behalf of the data subject.

Special rules regarding: children

Where the data subject is a person under the age of 16, he or she may still exercise his or her right of access if he or she has a general understanding of what it means to exercise that right. A person of 12 years or more is generally presumed to be of sufficient age and maturity to have such understanding. Therefore, if we receive a subject access request made on behalf of a child, we will need to use our judgment as to whether that child understands the nature of the request and, if we think he or she does, we should respond directly to the child. If we think the child does not understand, then we should send the response to the parent, guardian or other person authorised to make the subject access request on behalf of the child.

Special rules regarding: mentally and physically incapacitated adults

An agent may also make a subject access request on behalf of a mentally or physically incapacitated adult who is incapable of making his or her own decisions or incapable of

making a subject access request himself or herself. In this case, you should obtain from the agent either (i) a copy of his or her enduring power of attorney showing that he or she has been appointed to act as the data subject's agent, or (ii) evidence that he or she has been appointed by the Court of Protection to manage the property and affairs of the data subject.

10 Exemptions to the right of subject access

In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

10.1 Crime detection and prevention

We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we are able to.

10.2 Confidential references

We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

— education, training or employment of the data subject,

— appointment of the data subject to any office; or

— provision by the data subject of any service.

The exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual, which means you must consider the rules regarding disclosure of third party data set out in paragraph 7 before disclosing the reference.

10.3 Legal professional privilege

We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

— **Advice privilege**: this covers confidential communications between us and our lawyers where the dominant purpose of the communication is the giving or receiving of legal advice;

— **Litigation privilege**: this covers confidential communications between us or our lawyers and a third party (such as a witness) where the dominant purpose of the communication is the giving or seeking of legal advice in respect of current or potential legal proceedings. The claim to legal professional privilege in litigation ends as soon as the case has been decided and, at that moment, the documents in the file which were subject to legal professional privilege become available if a subject access request is received.

10.4 Management forecasting

We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions and demotions.

This exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

10.5 Negotiations

We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the data subject where doing so would be likely to prejudice those negotiations.

11 Deleting personal data in the normal course of business

The information that we are required to supply in response to a subject access request must be supplied by reference to the data in question at the time the request was received. However, as we have 40 days in which to respond and we are generally unlikely to respond on the same day as we receive the request, we are allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data are supplied provided that such amendment or deletion would have been made regardless of the receipt of the subject access request.

We are, therefore, allowed to carry out regular housekeeping activities even if this means that we delete or amend personal data after the receipt of a subject access request. What we are not allowed to do however, is amend or delete data because we do not want to supply the data to the data subject.

12 Multiple subject access requests

Where a data subject makes repeated and unreasonable requests for access, we are entitled to require that a reasonable period of time elapses between such requests. If, however, the data are altered frequently, then it will be reasonable for the data subject to make more frequent requests. Whether or not frequent requests are unreasonable needs to be determined on a case-by-case basis.

13 What happens if we fail to comply with a request?

If we fail to comply with a subject access request, or fail to provide access to all the personal data requested, or fail to respond within the 40 day time period, we will be in breach of the Act. This may have several consequences:

13.1 the data subject may complain to the Information Commissioner and this may lead the Commissioner to investigate the complaint. If we are found to be in breach, enforcement action could follow; and/or

13.2 if an individual has suffered damage, or damage and distress, as a result of our breach of the Act, he or she may take us to court and claim damages from us; and/or

13.3 a court may order us to comply with the subject access request if we are found not to have complied with our obligations under the Act.

14 Contacts and responsibilities

This Guidance will be reviewed periodically by the Authority's Data Protection Officer.

Any questions regarding this Guidance should be addressed to the Authority's Data Protection Officer.

Issued: February 2008
Version 1