Community Services: Education

Argyll House
Alexandra Parade
Dunoon PA23 8AJ

To: Heads of all Educational Establishments

Dear Colleague

Data Protection Act 1998

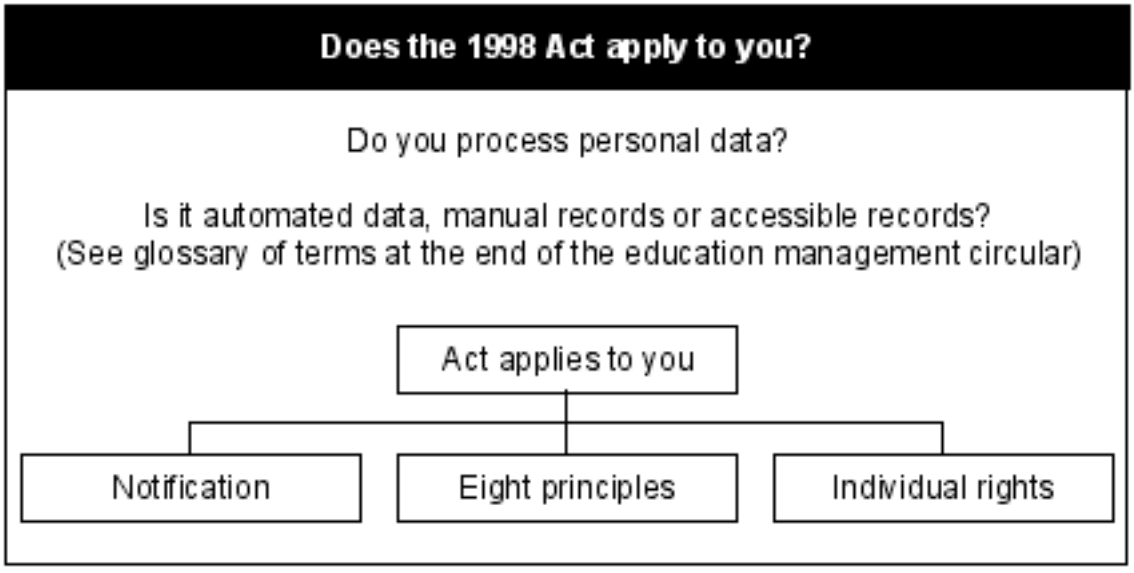
What is the Data Protection Act 1998?

The Data Protection Act 1998 came fully into force on 24 October 2001.

The Act repeals the Data Protection Act 1984. It also repeals the old Access to Personal Files Act. The new Act fundamentally governs the way we process personal data on living identifiable subjects.

Who does it apply to?

The Act applies to any person or organisation which processes any personal information on living identifiable individuals. Personal information can be held in a case file, assessment or report or simply in a notepad etc.



If we can say that the Act applies, then we need to observe the three requirements listed above:

- We need to have submitted **notification** with the information commissioner. This is where we state the purpose for which we process personal data, who the sources of data are and who has access to this information. Argyll and Bute Council's Data Protection Officer is responsible for submitting the notification.
- We need to observe the **eight principles** of the Data Protection Act 1998. These are explained further in this guide.
- We should pay particular attention to the **individual rights** of people on whom we hold personal data.

What is personal data?

Personal data is information we process about living identifiable individuals. Processing refers to anything we could possibly do with data, in whatever form it takes, be it manual files, written/typed documents, computer files, card index systems etc.

How we obtain information, how we record, hold, organise, adapt, alter, retrieve, share and delete - and the list goes on; anything we do with data involves some kind of processing.

What types of data do we have?

Data can be in different formats, but if it is relating to living identifiable individuals it is protected and governed by the 1998 Data Protection Act.

If an individual has deceased, the 1998 Data Protection Act no longer applies and we have no legal obligation to provide access to such files. Argyll and Bute Council owes a duty of confidentiality to data subjects and this continues after the death of an individual.

Examples of automated data: **computer files**, stored on floppy disks, CD-ROMs, DVDs, hard disks, backup tapes etc; **audio/video** includes CCTV images from security cameras, web cameras etc; **digitised images**, scanned images, digital camera images etc.

Examples of manual records: **employee/child or young person files**, personal data in written/typed format for identified individuals; **card index systems**, names, addresses, contacts etc; **microfiche records**, information transferred to this format is still a manual record on individuals or contacts etc.

Good information handling: the first principle of good information handling

This first principle requires that data controllers process personal data fairly and lawfully. Processing covers obtaining, recording, retrieval, consultation, holding, disclosing and use of data. Data controllers must not process personal unless at least one of the following conditions are met:

- the individual has given his or her consent to the processing;
- processing is necessary for the performance of a contract with the individual;
- processing is required under a legal obligation;

- processing is necessary to protect the vital interests of the individual;
- processing is necessary to carry out public functions;
- processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

The Data Protection Act imposes further restrictions on the processing of sensitive personal data which include information about racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal allegations, proceedings or convictions.

Fairness in process

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

- the identity of the data controller;
- the identity of any nominated representative for the purposes of the Act;
- the purpose(s) 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 is 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 the data controller from the overriding duty to process personal data fairly and lawfully.

Making the person aware that we hold information about them and the purpose for which we hold that information will ensure that we comply with *The Fair Processing Code* under the first principle.

What we should also think about here is:

- where did we get our information?
- how did we get this information?
- for what purpose do we require this?

Data protection principles

There are eight principles in the Data Protection Act, all of which help to guide and have an impact on the way we process our information.

Principle 1: personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- at least one of the conditions in schedule 2 (see below) is met; and
- in the case of sensitive personal data, at least one of the conditions in schedule 3 (see below) is also met.

In most cases this now means that, unless we are protecting the vital interests of the data subject or can prove necessity for having or using information, we require explicit consent for processing data on physical/mental health or condition, sexual life and ethnicity.

Schedule 2 conditions

Most education processing will be on the basis of statutory/public functions.

The conditions within schedule 2 include: consent, fulfilment of a contract, legal obligations, protecting vital interests, public functions and legitimate interest. One or more of the above conditions in schedule 2 must apply when processing personal data.

Schedule 3 conditions

The conditions in schedule 3 include: explicit consent, employment rights/obligations, vital interests, legitimate club use, in public domain, public functions, legal proceedings, health professional. At least one of the above conditions in Schedule 3 must apply when processing sensitive data.

A further amendment to data protection is the **Processing of Sensitive Personal Data Order 2000** (Statutory Instrument 2000/417) which gives extra schedule 3 conditions, for example, crime prevention/detection/prosecution.

Principle 2: personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

What purpose does this information serve? It should be used for this and nothing more.

Principle 3: personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Do you have enough information - or too much? Does it help you facilitate for your clients' needs?

Principle 4: personal data will be accurate and, where necessary, kept up to date.

Are your files up to date? Does the information accurately reflect the situation?

Principle 5: personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Have we fulfilled our legislative obligation? Should this file be marked for archiving?

Principle 6: personal data shall be processed in accordance with the rights of data subjects under this Act.

Do you know what access rights your client has? Are you familiar with the Subject Access Guidelines?

Principle 7: appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.

Your login details should only be known by you. What do you do if you accidentally lose information?

Principle 8: personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects, in relation to the processing of personal data.

Are you aware of the procedures you should follow if you are transferring or sharing information?

The case for consent

When working within our capacity as staff of the education service, providing a service to an individual, we do not always require consent to process information relating to them (implicit consent). This is the case where there is no likelihood of a significant adverse effect on the individual as a result of processing their information. We do have an obligation to inform data subjects that we hold information on them and why. They have a right to object to this processing if they so wish.

Where consent needs to be sought, eg when sharing information with another department, 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, given under duress or on the basis of misleading information, be deemed valid. Even where consent has previously been given, the data controller cannot assume that this will endure forever and individuals must be allowed to withdraw consent at any time 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.

There are several joint protocols which the education service will be involved in. It is understood that the Scottish Government will be issuing standard guidance for local authorities on the development of joint protocols.

How does this apply to the education service?

As a department we are in contact with many individuals on whom we process information. This information is held in two ways:

- a manual file; and
- on computer (eg SEEMIS) systems.

However we record information on individuals, data protection principles apply. Any information we have that is identifiable to an individual, no matter the format, is governed by the Data Protection Act.

Awareness

Staff should become aware of, and gain a good understanding of:

- the data protection principles, in this education management circular;
- subject access guidelines;
- security and confidentiality guidelines;
- protocols related to sharing information with other departments and agencies;
- where to find further information, or whom to speak to in relate to data protection and subject access.

What is our responsibility towards the Data Protection Act?

If your job entails recording or sharing any information about any living identifiable individuals then your responsibility is to ensure that what you record or share and how you do it, is in compliance with the data protection principles.

The next time you write in a file or add an observation in an ICT system or communicate information to another agency or person, it might help to think about the following question: "Is the data I am about to record or share …"

- processed fairly and lawfully?

- obtained and used only for specified and lawful purposes?
- adequate, relevant and not excessive?
- accurate and, where necessary, kept up to date?
- kept for no longer than necessary?
- processed in accordance with the individual's rights (as defined)?
- kept secure?
- transferred only to countries that offer adequate data protection?
- authorised to be shared with a third party? Or do I require further consent?

What to do if

Another person/agency (not the data subject) asks for information about an individual.

There are a few questions you need to have answered.

1 Can you positively identify who is asking for the information?

2 For what purpose do they need this information?

3 Is this a subject access request?

4 Is there a current protocol or other legislative agreement in place between ourselves and this person/agency to allow sharing of information?

5 Do we need explicit consent from the data subject to share this information?

6 Do I require authorisation from my line manager to give this information out?

7 Should I record this information request somewhere?

Consent is required from the data subject.

If you have answered the questions above and have verified that explicit consent is needed, has consent been given already? If not …

1 how do I get this?

2 how do I verify identification of the data subject signature?

3 where should I record this consent?

4 where can I get further advice?

A subject access request is received

The first thing to do is direct the request to your head of establishment or appropriate supervisor. From this point the procedures will be followed and an identified access worker will be allocated if the access request is to be processed.

In any instance if you are unsure about anything related to data protection and access rights you should always seek further advice from your line manager. They should be

able to advise you of the steps needed to ensure compliance with the Data Protection Act.

Further information on data protection matters is available from the data protection contact below:

Chris Shirley (Quality Standards Manager)
Education, Argyll House, Alexandra Parade, Dunoon PA23 8AJ
E-mail chris.shirley@argyll-bute.gov.uk
Phone 01369 708528

A glossary of data protection terms, and further guidance on procedures for dealing with subject access requests are attached.

Yours sincerely

Executive Director of Community Services
March 2010

Data protection glossary of terms

As a local authority holding electronic and manual files about our users, we are bound by certain legislation in the way we both record and share that information. The Data Protection Act 1998, which we need to follow, contains broad principles. The Data Protection Act now also covers access to personal files by users.

Other legislation that will have an impact on our information includes The Freedom of Information (Scotland) Act and The Human Rights Act. In following the government's modernisation agenda we will require to share some of our information with other professionals and authorities.

Below are some of the terms and their meanings as referenced throughout the Data Protection Act 1998 and this education management circular.

Data controller	Argyll and Bute Council.
Data user	All Education staff who access and use files/records for employees, children and young people.
Data processor	The parties processing data on our behalf.
Data subject	Individual(s) on whom we hold information.
Data processing	Processing is a generic term used within the Data Protection Act as it accurately covers anything we may require to do with client information, be it recording, storing, sharing or deleting. As data users we process information in various ways.
Manual record	Could be a case file or sticky note, diary notes, notepad etc. If it is identifiable to a living individual, it is a record.
Accessible record	A record that is identified to a living individual in a structured format, eg case file, microfiche record.
Structured record	Part of an accessible filing system.
Implicit consent	Where consent can be implied as a result of working within an education role, performing a legal statutory function; it is not always necessary to seek explicit consent
Explicit consent	In the case of information sharing with other authorities, we may require explicit consent.
Schedule 2 or 3	Lists of conditions that apply to data protection principle 1.
Subject access	Client/data subject requests access to their file.

Data Protection Act 1998: subject access request procedures

1 Introduction

1.1 Purpose of the guide

This guide is intended to provide an outline of Argyll and Bute Council procedures for processing subject access requests in compliance with the Data Protection Act 1998 and associated legislation.

Guidance on the freedom of information legislation is available form the Council website at http://www.argyll-bute.gov.uk/fofi.

If you are in any doubt over the procedure to follow or need advice on how to handle queries from members of the public or staff, you should contact (a) your line manager, (b) data protection service representative or, (c) Stephen Doogan, Data Protection and Information Security Administrator for advice.

1.2 Background to the Act

The Data Protection Act 1998 ("the Act") came into force on 1 March 2000. The Act is concerned with the right of individuals to control what is done with their data, and provides individuals with a right of access to personal information held about them by an organisation or individual within it. A right to challenge the accuracy of data held is also created. Note that the terms of the Act relate to data held in virtually any form, and can include written notes and records as well as electronic data.

In simple terms, the Data Protection Act is: "the overall framework within which users of personal data will operate".

The Act gives rights to individuals about whom information is held, and imposes obligations on those organisations or bodies who hold that information. Individuals are entitled to place a 'subject access request' to access any (or all) information the Council holds on them.

A leaflet detailing the access rights of individuals (data subjects) is available on the Council's website and from all Council offices on request. Copies are also available in the Outlook Public Folders, staff intranet and from the Data Protection and Information Security Administrator.

1.3 Data protection policy

As part of its governance framework the Council has a data protection policy of which this document is a subsidiary part. The data protection policy imposes duties on all employees, elected members and third parties working for, or in conjunction with, the Council. The policy is applicable to all personal data/information processed by the Council. A copy of the policy is available as per the leaflet above.

1.4 Procedures

The subject access request procedure is a fundamental aspect of the Council's data protection policy, and will be reviewed by the Data Protection and Information Security Administrator periodically and submitted for ongoing approval to the Information Security Forum annually.

1.5 Access rights

The Act states that a data controller, ie Argyll and Bute Council, shall comply with a subject access request within **40 days** of receiving a validated request from a data subject or their representative. This means that the individual must be provided with access to all the information they are entitled to receive within the timeframe.

An individual has the right to:

- request that the Council provides them with any information held about them;
- be informed by the Council if no information is being held about them;
- be provided with any information that explains terms/codes/markers that are otherwise unintelligible. Thus, if the personal data contains codes or indicators that can only be understood by reference to a key, the individual has to be provided with a key to those terms;
- have any inaccuracies corrected or the personal information erased or destroyed, where the circumstances are appropriate. [This does not mean that the person or organisation holding the data is obliged to correct or delete data solely at the request of the individual. The individual must provide evidence of inaccuracy or give reasons why the information should be deleted. Where such evidence is not provided, the individual can request that a file note be added to, but not replacing, the alleged inaccurate data.]

2 Subject access procedures

2.1 Receipt of a request

2.1.1 Identifying a request

A request for access to personal information should be treated as a 'subject access request' under the Data Protection Act. The request need not specifically mention the Data Protection Act, it may just ask for access to personal data/information. Upon receipt of a formal, ie written, request for information, you should immediately pass the details on to the either your line manager, service data protection representative, or the Data Protection and Information Security Administrator as soon as possible so as to enable a decision to be made as to the best way to appropriately expedite the request.

2.1.2 Role of service representatives

Each department in the Council has a data protection representative; a list of these is available on the Intranet. To enable effective monitoring of progress and action, service representatives must inform the Governance Unit of any requests received and the date that the 40 days subject access process commenced.

Departmental data protection representatives will consult with the Data Protection and Information Security Administrator as to how to progress subject access requests and may choose to pass the request on to another member of staff within their service to administer. However, they remain responsible for ensuring the information held by their service is collated, filtered and distributed within the statutory timeframe, and for ensuring the Governance Unit are informed of progress.

2.1.3 Requests made by Council employees

Internal subject access requests made by an employee or elected member in respect of their own personal information relating can be made directly to the Data Protection and Information Security Administrator, or via the relevant personnel section as appropriate. These will be dealt with in the same way as any other subject access request.

2.1.4 Requests made on behalf of another person

It is not uncommon for the Council to receive a subject access request from an individual on behalf of another person, eg parent requesting on behalf of their child or solicitor on behalf of a client. In each instance care must be taken to ensure that the individual has given consent to the other person to act on their behalf. If explicit consent is not shown, you should write to the applicant enclosing a mandate for the appropriate individual to sign and return to you before proceeding with the request. The 40 day "clock" stops until this issue is resolved.

There is separate guidance available to elected members regarding the personal information which they can access; if you have concerns about any aspect of this, you should contact your service data protection representative, or the Governance Unit.

2.1.5 Checklist upon receipt of a request

Details	Section
Has somebody asked for access to their personal information?	2.1.1
Have you passed the details onto your service's data protection representative?	2.1.1
For data protection representatives only: Have you consulted with the Governance Unit re the request?	2.1.2

Does the request require explicit consent (a signed mandate) from the data subject before it can proceed?	2.1.4

2.2 Processing of a request

Complex or multi-service requests will almost always be co-ordinated by the Data Protection and Information Security Administrator, but in his/her absence, or following discussions with the departments, this may be devolved to services as appropriate, with advice being provided as required.

The process described below outlines current practice, and departures from it should be documented and justified.

2.2.1 Timescale for complying with a request

The Council is obliged to satisfy subject access requests within 40 calendar days. The 40 days starts only when you have received sufficient details of the request, proof of identification of the requestor, and fee (where appropriate).

On receipt of a subject access request an acknowledgement should be sent to the data subject, informing them of the Council's understanding of the information they have requested, who will be responsible for processing their request, and the date that the subject access request commenced. A copy of this acknowledgement and the original request should be sent to the Data Protection and Information Security Administrator for monitoring purposes.

Mark the date on which the 40th day falls, so that you know the timeframe you are working around.

2.2.2 Fee

The statutory fee is £10 per request made and is payable in advance. Cheques should be made payable to "Argyll and Bute Council". For those unable to pay by cheque, cash payment will be accepted at any of the usual cash receipting points. Services are <u>not</u> permitted to charge photocopying costs on top of the £10 fee.

The Council has the right to waive the fee where appropriate. This decision should be taken on a case by case basis, bearing in mind that the Council has adopted a policy on charging. Any decision not to charge should be the exception rather than the rule.

2.2.3 Verification of identity

Acceptable identity documents include passport, driving licence and birth certificate; only one document needs to be provided. Data subjects should bring documents into a Council office; staff should photocopy the documents, verify any photographs and enclose the copies with their name, designation and date. Alternative arrangements may be made with the data subject on a case by case

basis, but this should be identified, recorded and checked at the time the original request is submitted to the Data Protection and Information Security Administrator.

2.2.4 Starting the search

Contact all the primary users in your service where personal data is held and request a full copy of any data held about the data subject. Remember, personal data may come from several sections in each service, so ensure that all areas are covered. Explain that there is a statutory time limit and that they should provide you with a response within 2 weeks.

Ask them to provide you with copies of all information they have on the individual, including emails, screen dumps from computer systems and written notes. If the employee does not retain any information on the individual, they should inform you of this fact.

2.2.5 Information contained within multiple services

If a letter/form has been received and requests all data held by the Council, or where it is possible that there may also be data held by another service, contact the data subject requesting clarification of which services are likely to hold data and in what connection. The standard access request form may be helpful in this regard.

The data subject is entitled to access all data but it is possible they are looking for specific information, and this may help to narrow the search.

If more than one service is involved, deal with the request within your service, but additionally, send a memo to the data protection representative in any other service involved, and copy it to the Data Protection and Information Security Administrator. Your service will still be required to co-ordinate the response.

If it is realised that it is likely that you are going to exceed the 40 day limit and not all data has been received from other services or third parties, notify the individual of any potential delay and the reasons for it. If possible discuss with them any urgent requirement for specific data to see if this can be supplied.

2.2.6 Checklist for processing a request

Details	Section
Have you received sufficient details of the request to proceed?	2.2.1
Have you received a fee and proof of identity?	2.2.2 2.2.3
Did you complete a subject access request acknowledgment form and send this out to the data subject?	2.2.1

Was the subject access request acknowledgment form copied to the Information Security Team?	2.2.1
Have you taken a note of the date on which the 40th day falls?	2.2.1
Have you contacted all the primary users in your service and asked them to return all data to you by a specified date?	2.2.4
If the initial request is "for all information you hold on me", have you sent a letter to the requestor asking them to identify what services are likely to hold data on them?	2.2.5
If more than one service is involved, have you sent a memo to the other services with details of the request?	2.2.5
If you are about to exceed the 40 day limit, have you informed the data subject of the delay and informed them of an estimated response time?	2.2.5

2.3 Receipt of data

When all the data for the subject access request has been collated, it must be filtered (ie redacted) before it is provided to the data subject.

If no personal data exists (or if you are relying completely on an exemption) you must still notify the individual that no personal data exists or that you are relying on a stated exemption, within the 40 day time limit.

2.3.1 How to prepare a file prior to disclosure

(a) Review the file to see if it contains any 'third party' data and, if so, redact (2.2.3)

'Third party' means information identifying an individual other than the data subject. This could include their partner, parents, siblings, children, neighbour or similar, but does not include employees of the Council acting in the course of their duties. As noted above, in many instances it will be necessary to remove certain data from files prior to release to balance the competing interests of the data subject and the legitimate privacy concerns of others. The specialist guidance notes from the ICO [Information Commissioner's Office] on dealing with subject access requests must be fully understood prior to undertaking this task.

(b) If the file does contain third party information, permission may need to be sought for the applicant to see this information

In many instances it will be clear from context that third party information is already known to the data subject eg it was supplied by them, or that the third party makes reference to the data subject's knowledge. Similarly there may be

occasions where it is extremely unlikely that the third party is would give consent to disclosure.

You should consider whether it is necessary or appropriate in the particular circumstances of the case to obtain the third party's consent, and if so write to them enclosing a consent form and stamped self-addressed envelope.

Where the third party fails to reply to the request or consent is refused, contact Legal Services or the Governance Unit to clarify whether it is reasonable in the circumstances to disclose the information without consent.

When it is not possible to contact the third party, all identifying information should be redacted, ie blocked/blanked out.

(c) Category E

Most data controllers are able to fulfil their data protection obligations by ensuring that all data held within their "relevant filing systems" is accessible to a person making a subject access request. Local authorities, however, require to go further in the form of providing access to category E data. This is personal information which is recorded by the authority but is not part of a relevant filing system. It can be in any form, including electronic data, images, paper files or documents. It does not have to be held in a database or filing system and will include recorded information held in a manual, 'unstructured' form by a public authority, eg the paper file on or in your desk.

Essentially any reference to an individual in any document or other information held by a public authority can be personal data.

(d) Review the file to remove any information considered to fall under "legal professional privilege"

Legal professional privilege relates to information between a lawyer and client (member of staff) which constitutes legal advice.

If you are unsure whether information within a file may constitute legal professional privilege you must contact Legal Services or the Governance Unit.

(e) Provide a key to explain any codes or markers

If any of the information is held in a coded form, you must provide a key to the codes used and give full explanations describing what the use of each code means.

(f) Maintain a record of information that is released or withheld from access

You must maintain a record of the information that the individual has had access to. If the file is relatively small, ie one A4 ring binder, you should

photocopy all the information that the individual has had access to, and retain this copy on file along with details of the request. If the file is too substantial to photocopy, you must retain a record of the information that has been provided or exempted. This could be by cataloguing each document showing a description of the document, the date of the document, and whether it was released to the individual or not; see a specimen at the end. Or it could be by indicating that the entire file was provided, with the exception of specific recorded data. eg all pages where any redaction was performed. What is required will vary on a case by case basis. This record must be held as securely as the original information itself; it will, in practice, often be held as part of the main file once completed.

2.3.2 Provision of data to law enforcement bodies

It is sometimes suggested that section 29 of the Data Protection Act requires data controllers, ie the Council, to provide information to law enforcement bodies. This is incorrect. Section 29, in common with all the other exemptions in the Act merely allows the data controller an exemption from the obligation to process the data fairly, thereby providing an opportunity to disclose if the processing (ie the disclosure) is taking place for the purposes of the prevention and detection of crime.

If the data controller is satisfied that the processing is for this purpose, then (s)he can claim the section 29 exemption, but the data subject's right of redress should the data have been inappropriately disclosed remains with the data controller.

While some legislation may contain disclosure provisions, eg Protection of Children (Scotland) Act, there is never any obligation under the Act to provide personal data without a court order. If you are being asked to disclose information to anyone other than the data subject themselves, you should always seek advice either from Legal Services or the Governance Unit.

2.4 Providing the information

2.4.1 Responding to the subject access request

There are several options for providing the information to the data subject. This should, where appropriate, be agreed with the data subject.

2.4.2 Contact details

Ensure you have provided the individual with a contact or reference point within your organisation should they wish to discuss any of the information they have received from you as part of their subject access request; this will usually be the same person who co-ordinated the request, but may, for example, be a social worker or other professional officer.

2.5 Subject requests by the same individual

Under the Data Protection Act you are not obliged to comply with a request that has been made too soon after compliance with a previous request. While there is no definition of what a reasonable time might be in the legislation, a year is generally regarded as the minimum, unless substantive changes have taken place more frequently, which may happen dependent on the nature of the information. Decisions must therefore be made on a case by case basis.

If a subsequent request is made, the service should provide any information they hold *from the date of completion of the first request*. For example, if the individual has made a subsequent request on 30 April 2010, and their previous request was completed on 31 December 2009, you need only supply the information from 1 January 2010 to 30 April 2010. If the individual was to request another copy of the information held previously, you should have a record and/or photocopy on file of what was disclosed earlier.

2.6 Complaints

If the individual is unhappy with the response, an attempt should be made to resolve the matter within the service initially. Thereafter complaints will be dealt with under the corporate complaints procedure. The individual has the right to complain directly to the Information Commissioner at any time.

Support contacts

Stephen Doogan	Data Protection and Information Security Administrator	Stephen.Doogan@argyll-bute.gov.uk	4323
David Sinclair	Risk Management Assistant	David.Sinclair2@argyll-bute.gov.uk	

Specimen

Example 1: detailed record of information that has been provided / exempted during a subject access request, and the reasons for exemptions.

Subject access request: information contained within John Smith's file			
Ref	Description	Date of document	Copy provided to subject?
Case file 1			
1.1	Email from (Community Care) to (Legal) requesting verification of attached draft letter to Mr Smith and welcoming changes.	26/01/04	Email: yes Draft letter: no
1.2	Email from (Community Care) to (Legal) advising they had received a letter of complaint from Mr Smith and enclosing Community Care's reply for information.	12/11/03	Yes
1.3	Letter to Mr Smith from (Community Care) replying to Mr Smith's letter of 11/11/03.	14/11/03	Yes
1.4	Initial assessment and screening forms (IAS).	07/01/04	Yes
1.5	Care Plan (CCM2) (3 page document).	14/02/04	Yes
1.6	Email from (Legal) to (Community Care) advising on guidance received from the Scottish Executive concerning an ongoing complaint.	28/03/04	No: legal privilege, exempt
1.7	Contacts summary and action sheet (11 page document).	29/03/04	Yes, but third party ref removed (P2, 22/01/01)
1.8	Email from (Community Care) to (Community Care) re telephone call from (a neighbour) of Mr Smith.	08/04/04	No; third party, exempt
1.9	Out of hours service fax to (Community Care) advising there was not enough staff to visit Mr Smith.	16/04/04	Yes
Case file 2			
etc	etc	etc	etc