



Management CIRCULAR No.

87

July 2005
Management Circular No. 87

Glasgow City Council
Education Services
Wheatley House
25 Cochrane Street
Merchant City
Glasgow G1 1HL

To **Heads of all Educational Establishments**

Dear Colleague

Designing a School Web-site

Introduction

The World Wide Web is made up of lots of web-sites. A web-site is a set of pages stored on computers linking around the world. It brings together a community of large and small companies; schools and colleges; libraries and any number of individuals. The prime purpose of any web-site is to provide information. Having a school web-site can provide information for existing pupils and parents/guardians or promote the school to prospective ones. The site can be used to showcase examples of pupils' work, to share resources for teaching and learning at school and with colleagues elsewhere.

An ever growing number of schools have already developed highly sophisticated and award winning sites of which the pupils and staff are rightly proud. However schools, having little or no experience in web-site construction, have increasingly been seeking advice on building a school site. Education Services have been working in partnership with Continuing Education Gateway to provide a web-site template that is now available for schools to use.

This Management Circular aims to provide some essential advice on web-site publishing and outlines how the Gateway template may be used.

Education Services wishes to host all school web-sites on the servers provided by Gateway and to ensure that all school sites are associated with the *glasgow.sch.uk* domain. This does not require all schools to use the template provided by Gateway, but does require all schools to ensure that, when existing hosting contracts have expired, sites are transferred to the Gateway servers. For information on the procedures for transferring to Gateway servers see Appendix 1.

If you would like further information about Gateway's template web-site, please contact:

Continuing Education Gateway
199 Nithsdale Road
GLASGOW
G41 5EX
Phone 0141 422 1070
Fax 0141 422 2006
E-mail schools@ceg.org.uk
Web-site www.ceg.org.uk

Policy Statement

Glasgow City Council's policy on Information and Communications is specific in four related areas and all sites must comply with these. They are:

1. Do not disclose confidential information unless you are sure the web-site is using appropriate security;
2. No messages may be posted on any Internet message board, newsgroup or other similar web based service that would bring Glasgow City Council into disrepute, or which a reasonable person would consider offensive or abusive. Remember, even though you may not leave your name, other identification methods exist which may still allow others to locate the organisation that you work for and the particular computer used to post a message;
3. When using newsgroups, actively disclaim that you are speaking for Glasgow City Council unless you are acting as an officially recognised spokesperson;
4. FTP transactions and Java based downloads can compromise Glasgow City Council security policies. These must only be undertaken under ICT supervision on equipment isolated from all servers;

Every web-site should carry a copy of the Glasgow City Council Copyright, Disclaimer and third party links statements available as Appendix 2 of this Management Circular.

Site Content

Education Services request that every school web-site contains the following information and that this detail is regularly reviewed and updated.

Information	Detail
Introduction by the Head of Establishment	A brief, clear and simple statement of the aims and objectives of the school
School Contact Information	Postal address, phone and fax number and e-mail headteacher@schoolname.glasgow.sch.uk
School Roll	Present roll at each stage including any Nursery accommodation
Denominational Status	Roman Catholic/Non-Denominational
School Hours	Start time, interval times and finish time
School Year	Holidays and in-service days
Enrolment Procedures	Who to contact and when
Curriculum	Details of the curriculum which is being taught in the school
Associated schools/nurseries in the community	You could include information on the New Learning Community
Breakfast Club	Time of Breakfast Club and any activities which are also provided
After school activities/sports clubs	Days and times of clubs which are provided through the school
School safety	School security/getting to school/road safety

Standards for Web-site Development (the seven C's)

Involve both staff and pupils when developing/gathering information for the site. The following advice is offered as a basis for planning the content of a school site.

The content must be:

1. Correct	Check the information posted on the site is factually correct
2. Cohesive	Use consistent house style such as font/colours/line spacing etc. This makes it easier for the user to use/identify Check information flows in a logical manner
3. Concise	Less is more. Don't populate the site with irrelevant details Keep it simple
4. Current	Update the site regularly Archive out of date material. Keep the site fresh
5. Clear	Give pages a title. This makes them easy to identify Keep language and presentation plain and simple. As a variety of people will visit and use the site, avoid jargon and acronyms Do not use backgrounds or fonts which make content difficult to read
6. Careful	Check you have parents'/guardians' permission to include children's work/ photographs/input to the site Check copyright Web-sites SHOULD NOT include personal details or names of any child or adult in photography, personal e-mail/postal addresses or phone/fax numbers
7. Collaborate	Collaborate with SMT, staff and pupils to decide: Aims and objectives How the site will reflect the ethos and values of the school Accept/reject material. Suitability/appropriateness and quality issues Time for development/maintenance of site. Who will update the site? Who will manage the project? Who is responsible?

Corporate Communications Statements

To ensure consistency and quality throughout all school web-sites the following guidelines must be adhered to:

Content

A list of minimum contents (Page 2) has been established. This is the basic information about the school. If this information is not available, then the Head of Establishment should not authorise the web-site to go live.

Updating

Schools have the responsibility to ensure that all information published on their web-site is updated on a regular basis.

Corporate/Political Information

Any information on the web-site which refers to Council policy or political issues must be approved by Education Services Directorate.

Issues of Safety

It is the duty of the school management to ensure that every child in their care is safe. The same principles should apply to the virtual presence of a school as would be applied to its physical buildings. Schools must ensure that no individual child can be identified or contacted either via, or as a result of, a visitor using the school web-site.

Advice on safety issues can be obtained at:

- www.ltscotland.org.uk/ictineducation/ictadvice/internetsafety.asp
- www.scotland.gov.uk/clickthinking/default.htm
- safety.ngfl.gov.uk/schools/document.php3?D=d72

Images of Pupils

Including images of pupils on the school web-site can be motivating for the pupils involved and provide a good opportunity to promote the work of the school. It is important to balance the potential risks of including images of pupils on the web-site against the design principles of creating colourful, attractive and relevant pages, as the school SMT would do with any publication.

Schools need to develop a policy in relation to the use of images of pupils on the school web-site. The SMT and site administrator will need to make decisions about the type of images they consider suitable and that appropriately represent the school. They will want to ensure parents/guardians support their policy. When assessing the potential risks in the use of images of pupils, the most important factor is the potential of inappropriate use of images of children.

Do not use the names of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school.

Schools may want to include images of an individual or a group of children who have won a competition or who have been involved in a school trip. Avoiding naming pupils who feature in the image reduces the risk of inappropriate contact.

An easy rule to remember is:

- i. If the pupil is named do not use their photograph;
- ii. If the photograph is used avoid naming the pupil;
- iii. If in doubt, leave it out.

Ask for permission to use an image of a pupil. This ensures that parents/guardians and pupils are aware of the way the image is being used to represent the school. The **Parental/Guardian Consent Form** (Appendix 3) should be used for this purpose.

To reduce risks to pupils, there should be recognised procedures followed to ensure that inappropriate material is not used on a web-site.

The school should therefore:

- i. Be cautious about publishing pictures of pupils, and ensure that this only happens in line with Glasgow City Council policy. Ensure that the appropriate permissions are obtained;
- ii. Not identify pupils by name or give their e-mail addresses;
- iii. Only use images of pupils in suitable dress to reduce the risk of inappropriate use;
- iv. Have text written by children checked by a member of staff before publication as it may include potentially problematic material such as personal information or defamatory statements. Children should be encouraged to think carefully about what they say;
- v. Have a member of staff check any additions or amendments to the school site before it goes live. This should include checking any links placed on the site and these should be regularly reviewed

IF IN DOUBT LEAVE IT OUT

Accessibility

Gateway's schools web-site template will be assessed by Bobby software. This is a comprehensive web accessibility software tool designed to help expose and repair barriers to accessibility and encourage compliance with existing accessibility guidelines. A Bobby approved rating for all school sites will be aimed for.

This software will assess the general design of the site and the sections to be populated by schools should take account of the following Royal National Institute of the Blind (RNIB) advice:

"Individuals with cognitive or sight problems may have difficulty reading and distinguishing text from a background colour. This is generally caused by poor choice of colour and contrast in the design of the page. Background images and patterns may also cause problems of legibility". For further information please visit: www.watchfire.com/products/desktop/accessibilitytesting/default.aspx

What to avoid

- i. Use of dark backgrounds and dark text. For example, red on black or green on red;
- ii. Use of light text on a light background. For example, white text on pale grey ;
- iii. Use of complex backgrounds, such as images and patterns, which visually interfere and make reading the text difficult.

What to do

- i. Use high contrast colours for text wherever possible;
- ii. Creative use of colour and contrast can dramatically enhance the accessibility of a web-site. It can be as important for people with sight problems as it is to people who have dyslexia or whose first language is not the main language of the site;
- iii. Everyone benefits from text which is both easy on the eye and that is easy to follow. For example, people with dyslexia benefit from good contrast as this can help make the structure of words and sentences easier to understand;
- iv. Glasgow City Council advise the use of the following font and size for web-site construction:

Verdana – size 12

Data Protection Act 1998

The Data Protection Act 1998 states, that anyone processing personal data must comply with the eight enforceable principles of good practice. Further information regarding data protection can be found on the web-site of the Information Commissioner: www.dataprotection.gov.uk

- i. General information on the impact of the Data Protection Act for schools can be found on the ICT advice site:

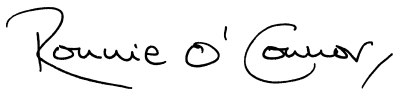
www.ictadvice.org.uk

- ii. Appendix 4 is a copy of advice issued by Glasgow City Council's Solicitor, dealing with Data Protection issues.

- iii. Appendix 5 is a copy of the advice on Data Protection matters issued by Glasgow City Council.

As previously stated, Continuing Education Gateway have developed a web-site template for schools to quickly develop a web-site. Appendix 1 provides relevant contact details.

Yours sincerely



Ronnie O'Connor
Executive Director (Education, Training and Young People)

Continuing Education Gateway Contact Information

Web-site Hosting for Glasgow schools

If your school has developed its own web-site or is planning to do so, Gateway will be pleased to host your web-site and ensure that it is available at all times, with any essential downtime kept to a minimum.

Costs

There will be a cost per annum for hosting and providing remote access for updating purposes. Gateway will provide estimated costs on request.

Information required by Gateway includes:

- contact details of the organisation currently hosting the web-site;
- an electronic copy of the web-site;
- information about the software used to develop the web-site; and
- contact details of the member of school staff, with responsibility for the site.

Web-site Template

If you would like further information about Gateway's template web-site, please contact:

Continuing Education Gateway
199 Nithsdale Road
GLASGOW
G41 5EX
Phone 0141 422 1070
Fax 0141 422 2006
E-mail schools@ceg.org.uk
Web-site www.ceg.org.uk

Copyright and Disclaimer Statements 2004

Copyright © (*school name*). All rights reserved.

Copyright

By viewing or accessing this site, you are acknowledging your agreement to the following statements:

- Unless otherwise stated, copyright and similar rights in all material presented on this web-site, including graphical images, is owned by (*school name*);
- All information relating to a third-party is for the purpose of providing the end-user with relevant information regarding the third-party and is not considered to be the intellectual property of (*school name*);
- You have limited permission to print or download extracts from these pages for your personal non-commercial use only
- No part of this web-site may be reproduced or transmitted to or stored in any other web-site, nor may any of its pages or part thereof be disseminated in any electronic or non-electronic form, nor included in any public or private electronic retrieval system or service without our prior permission;
- You may not create a database in an electronic or other form by downloading and storing all or any part of the pages from this site without our prior written consent save as expressly authorised by an agreement in writing between us;
- Any copies of the pages of this web-site that you save to disk or to any other storage system or medium may only be used for subsequent viewing purposes or to print extracts for personal use.

The structure and source code of the database and online functions integrated into this site are the sole property of Glasgow City Council (Continuing Education Gateway) and cannot be copied or published in any format or medium without our prior consent.

Links to Third Party Sites

This web-site contains links to the sites of third-party information providers. The information provided by these web-sites or subsequent linked web-sites is not within our control and is therefore not the responsibility of (*school name*). The inclusion of any link does not imply endorsement of the web-site by us.

Disclaimer

(*School name*) makes every effort to provide accurate and current information on this web-site. However, it does not give any warranty or representation of any kind with respect to the site or its contents, including warranties in respect of the accuracy, completeness, appropriateness or currency of the information on the web-site.

End-users should check with the relevant learning providers and other organisations represented on the web-site that information relating to them is accurate and current.

To the fullest extent permitted at law neither (*school name*) or its employees or pupils will be liable for damages arising out of, or in connection with, the use of this web-site.



Pupil Classwork and/or Photographs Consent Form

PLEASE USE BLACK INK AND BLOCK LETTERS

Pupil name

School

Classwork/photographs and any reproductions made thereof will be used solely for the purpose of promoting Education Services, which will involve the inclusion of classwork/photographs in the school web-site produced by Glasgow City Council Education Services and for no other purpose whatsoever. Photographs will be taken on behalf of Education Services Directorate.

Pupil's classwork/photographs and any other reproductions thereof will be used for a period of three years from the date on which the classwork/photographs are published on the school web-site.

NOTE: If, within the said three year period, you wish to withdraw this consent you can do so by writing to or phoning the school directly. Upon receipt of such request, you will be notified by letter, acknowledging receipt of request for withdrawal. The classwork/photographs or any reproductions thereof will be removed from the school web-site from the date of the said request. The classwork/photographs will then be destroyed.

Parent/Guardian name

Date

Address

Postcode

Parent/Guardian Signature

Relationship to pupil

Parent

Guardian

Other

(please specify) _____

Pupil Signature (Age 12+)

NOTE: Consent should be sought from pupils above the age of 12 in addition to their parents/guardians

FOR OFFICE USE ONLY

Location of photograph taken

Contact person

Date

Solicitor Advice Note

Data Protection (Glasgow City Council Solicitor)

The relevant rules are found in the Data Protection Act 1998 (“DPA”). Under Data Protection Act, photographs can be regarded as “*personal data*” and so taking and using photos falls under the Data Protection rules. These rules require us to satisfy certain conditions before we are allowed to process (e.g. acquire, use, disclose, etc.) personal data including photographs. One of the conditions is consent of the individual, so if the individual agrees, this is not a problem.

However, consent is not the only condition: another condition states that processing is permitted if it is necessary for the legitimate interests of the data controller (the person who determines the purpose for and manner in which data are processed, e.g. Glasgow City Council) or third parties to whom it is disclosed (e.g. pupils and parents/guardians who get a newsletter). I do not normally advise reliance on this provision as it is vague and potentially open to abuse but the circumstances of non-controversial photography, particularly of public events such as sports matches or shows, would seem to me to meet these criteria.

It still remains necessary to ensure the processing is “*fair*”. This includes telling the subjects of the photographs who the data controller is (e.g. Glasgow City Council) and explaining in general terms what the data will be processed for. I understand that many school handbooks have sections on photography. If these sections meet the above requirements, this would satisfy our legal obligations.

Please note that there are specific rules on sending personal data outside Europe, data protection being almost exclusively a European phenomenon. This includes posting photographs of identifiable individuals on a school web-site. Such photographs should **ONLY** be posted on a web-site with the consent of the individual. In terms of whether it is the parent/guardian or pupil who consents, the rules are that any child aged 12 or above is presumed to be old/mature enough to have sufficient mental capacity to be able to consent on their own behalf (which wouldn’t preclude a school from informing parents/guardians about what was happening but it does mean that you shouldn’t be asking the parents/guardians to consent when it’s the child’s consent that matters). Mature children of less than 12 may have sufficient capacity but this cannot be presumed and I would advise seeking parental/guardian consent for such children.

In relation to storage of photographs, there is a general requirement on organisations to take “*appropriate technical and organisational measures*” in relation to data security, although this is defined as measures ensuring a level of security which is appropriate, given the nature of the data and any harm which might otherwise occur. The security measures to be applied to photographs intended for publication probably therefore do not have to be quite as rigorous as for some of the other personal data Glasgow City Council processes. Assuming the Education network is reasonably secure and sensibly partitioned, it’s probably safer storing photos on a network drive than on a removable disk.

Data Protection Act 1998: Guidance for Staff

Introduction

The *Data Protection Act 1998* (DPA 98) gives effect in the UK to a European Union Directive on the free movement of personal data and completely replaces the Data Protection Act 1984 (DPA 84) and Access to Personal Files Act 1987 (including the Social Work and Housing Regulations made under that Act). It came into force on 1 March 2000, although most of the new rules have only applied from 24 October 2001.

Both DPA 98 and DPA 84 were intended to safeguard the privacy of individuals in the computer age. The DPA 84 was driven by a Council of Europe Convention (the same source as the European Convention on Human Rights). It is likely that compliance with DPA 98 will provide a defence to any alleged breach of the Article 8 right to privacy under the *Human Rights Act* in respect of the use of personal data.

Scope of Data Protection

DPA 98 essentially regulates the processing of personal data. "*Processing*" means doing anything at all - acquiring, disclosing, accessing, amending, deleting - even the fact of holding data amounts to processing. "*Personal data*" means data which relates to a living individual who can be identified from those data and/or other information in the possession of (or likely to come into the possession of) the data controller e.g. the Council. This covers not only automated records (as in DPA 84) but also manual records held in a "*relevant filing system*" (e.g. a filing system structured so that the information relating to a specific individual can be readily accessed). This extension of coverage to manual files clearly has significant implications for the Council's records management system, and extensive work will be required to ensure that file management systems allow us to comply with the Act. The Act can also apply to items such as recordings of telephone conversations, CCTV footage and still photographs, or reference to an individual in an e-mail or internal memorandum. Personal data may be as little as name and address (or either of them if the individual can be clearly identified) or it may be an entire file full of highly personal details.

It is essential that all staff are aware that individuals have an enforceable right to see the information the Council holds on them. There are very few exceptions to this rule. Accordingly, all staff should be aware that if they record anything about an individual, the individual will probably be able to see it. This includes internal e-mail messages about the individual.

The basic rules are as follows:

1. If you process personal data you require to have an entry (called a "*notification*") in a public register maintained by the Information Commissioner (formerly called the Data Protection Commissioner). The Notification for Glasgow City Council is handled by the Council's Data Protection Officer, who is located in Internal Audit and Inspection. The current notification can be viewed at www.dpr.gov.uk (no. Z4871657) or on Financial Services' intranet (Internal Audit/Data Protection). Additional Notifications cover the District Court, Licensing Board, Strathclyde Joint Police Board, the Assessor and Electoral Registration Officer and the Children's Panel/Children's Panel Advisory Committee. Do NOT respond to organisations (typically with names like "*Data Protection Registration Services*") which send in demands for money on the basis that your part of the Council needs to notify under the DPA. Such demands are probably illegal and should be forwarded instead to Consumer and Trading Standards in Environmental Protection Services.

2. The processing must comply with all eight Data Protection Principles found in Schedule 1 to the Act. These are attached as Appendix 1.
3. The first DP principle requires processing to be fair and lawful, and in particular requires that at least one “*Schedule 2 condition*” is met. Schedule 2 is attached as Appendix 2. Most processing by the Council will be covered by condition 5(b) or (d) (e.g. statutory or public functions) but note the caveat mentioned in Paragraph 5 below. “*Fair*” processing also requires a “*fair processing notice*” (also called an “*Article 10 notice*”) to be given to the data subject (or made readily available to them) at the point where their data are collected. This tells the data subject who is collecting the data and what it will be used for, as described under “*Other Rights of Data Subjects*” below. Getting the fair processing notice right is the easiest and best way to help ensure compliance with the Act.
4. In the case of sensitive personal data it is also necessary to satisfy a Schedule 3 condition (found in Appendix 3). “*Sensitive personal data*” means information relating to racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health, sexual life, and data about the commission or alleged commission of an offence or the disposal of criminal proceedings against someone. Again, Condition 7(1)(c) of Schedule 3 (processing necessary for functions under any enactment) will legitimise much Council processing but again, see the caveat below. Additional Schedule 3 conditions can be found in the Data Protection (Processing of Sensitive Personal Data) Order 2000. These additional conditions include processing which is necessary for the prevention or detection of any unlawful act.
5. Most Schedule 2 and Schedule 3 conditions require the processing to be “*necessary*” for the purpose in question. However, much of the processing carried out by the Council will be to improve service delivery and is not strictly “*necessary*” to meet basic statutory duties. In such cases, it will often be necessary to rely on the consent of the individual. This is best done at the outset, and the consent form can double-up as the fair processing notice.

It is necessary to comply with these steps each time the data are processed. Thus a disclosure of information to a different department must be checked for compliance, as must disclosure to outside agencies or the use of data internally for a use other than that for which it was originally acquired. For internal disclosures, the important question is the use which is being made of personal data rather than which Council Service or section is carrying out the processing.

Disclosure of Personal Data

Disclosing personal data to outside persons or organisations can be problematic. In each case, the disclosure has to satisfy all the rules mentioned above. When deciding whether to disclose data, the following points may be of assistance:-

1. Do you actually want to disclose the data? If you don't want to, then don't do it. Few organisations can compel the Council to disclose personal data which we wish to retain. Even under the *Freedom of Information (Scotland) Act 2002* (which came fully into force on 1 January 2005), there will be at best a very limited right to see personal data relating to other people. A number of other statutes requiring the Council to disclose information are noted below.
2. Does the data subject know or expect that you will make the disclosure? Most applications forms issued by the Council specifically advise that the information provided may be checked for accuracy or used in fraud detection/revenue maximisation data matching exercises. If the data subject has consented, then you can almost certainly disclose their details. Other cases may be less clear. A useful technique is to consider whether the person would have a reasonable expectation that we would not disclose the information to the party in question. In the absence of very strong factors in favour of disclosure, a specific request to keep personal data confidential should be observed. The Council does not keep personal data in order to act as a debt collector for private concerns, and in general requests for forwarding addresses, etc. should be refused unless from a public sector body (e.g. the Police) – see point 4 below.

3. Can we control the data after disclosing it? The Council might be happy to release data to an outside party for purpose A, but not be happy for that party to use it for purpose B. The Council only retains control of the uses of data once it has been disclosed if it has the agreement of the other party.

This can be done by means of a data-sharing Protocol, which helps to ensure that the disclosure is lawful by specifying which permitted purpose the data is to be used for. Legal Services can assist with the preparation of Protocols. This should be considered where there is a regular information exchange with an outside party. For one-off or ad-hoc releases, the standard request form spells out limits on the permitted use of the data released.

4. Has the request been made in writing? Standard disclosure request forms for use by the Police, H.M. Revenue and Customs, etc., have been prepared which specify a number of points the requesting agency need to satisfy us about. These forms should be completed before any personal data is released. A copy of the Standard Release Form is appended to this note.
5. It should be noted that following the housing stock transfer, the Glasgow Housing Association remains an external organisation. Disclosure to GHA therefore has to satisfy the normal rules, although there are a number of data sharing agreements between the Council and GHA covering most routine exchanges of personal data.

If processing is outsourced (e.g. if payslips were printed by an outside company), there will clearly be some release of personal data to the outside company. However, since the Contractor is acting purely as the Council's agent, and is not making independent use of the data, this doesn't really count as a disclosure at all. DPA 98 imposes a requirement to have a written contract regulating such "*Third party processing*". A pro forma contract can be obtained from Legal Services. It is essential to have a written contract in place for all third party processing.

Transfers of personal data outside the European Economic Area should, in general, only be made with the consent of the data subject. This applies to any personal details (including photographs) which are posted onto any Council web-site.

Finally, it is a criminal offence for a member of staff knowingly or recklessly to disclose personal data without the consent of the data controller e.g. the Council. Members of staff who are following Council policy or acting on the instructions of their line manager would be deemed to be acting with the Council's consent.

Rights of Data Subjects

Data Subjects (e.g. the people to whom the personal data relates) have far more rights under DPA 98 than previously. Almost all of these rights are subject to limitations and exceptions. The main right is that of subject access but there are others. The following description is only an outline.

Subject Access

You have the right to see the data held which relates to yourself. Response to a request must be made in writing within 40 days of receiving satisfactory proof of ID. A maximum fee of £10.00 may be levied (except for Education and medical records which have a different fee system). Council policy is to charge for CCTV requests; departments are otherwise free to decide themselves. All information held (unless exempt) must be provided irrespective of the cost or effort involved in locating and providing a copy of it. This clearly has potential resource implications. The response must consist of the data itself (plus explanations of any codes, etc., used), the purpose(s) for which they are/will be processed, the source of the data and any recipients/intended recipients of the data. The main exception is that you are not obliged to disclose information relating to another individual without that other person's consent. Such data should be censored out unless it is reasonable in the circumstances to leave it in. Information is exempt from Subject Access if it is processed for the purpose of crime detection and disclosure would prejudice that purpose. Other exemptions cover matters such as health and safety at work, confidential references and management forecasts, or legal advice.

Any request for personal data should be forwarded immediately to the Council's Data Protection Officer at 108 Ingram Street, Glasgow G1 1ET to enable him/her to collate the corporate response. Again, all staff receiving such requests should be advised of this need. It is not necessary for the request to mention data protection.

An exception to this procedure exists for requests for access to Social Work files, which have slightly different rules and are handled internally by Social Work Services. Requests to see housing files should, if the data subject agrees, be forwarded to the Glasgow Housing Association as they are now the data controller of tenants' files. Finally, there remain rules (recently reformulated – the *Pupils' Educational Records (Scotland) Regulations 2003*, SSI 2003/581) allowing parents/guardians to see their children's records without the child's consent. These parental/guardian rights run in parallel to the rights under DPA98. Subject access rights (and other Data Protection Rights) are those of the data subject, not the parent/guardian. The law presumes that children of 12 or above have sufficient capacity to exercise their rights under the Act. Parental/Guardian requests (without the consent of the child) should only be given effect to if the child lacks mental capacity, and even then may be refused if the request is not the bona fide exercise of parental/guardian rights and responsibilities.

Subject access only gives a right to see your own data, so it is essential that the applicant's identity is confirmed prior to giving effect to a subject access request. Information relating to a third party which is found in the data subject's file should, in general, be removed before the file is released: There are, however, exceptions to this and advice should be sought.

Other Rights of Data Subjects

1. Subject Information Notices - "*Article 10/Article 11 Notices*": Fair processing requires that a Data Subject has, is provided with, or has made readily available, certain information. This information consists of the identity of the Data Controller, the purposes for which the data are intended to be processed, and any other information which is necessary in the circumstances to allow the processing to be fair. An "*Article 10 Notice*" is where the information comes direct from the Data Subject, and an "*Article 11 Notice*" is where it comes from a third party (they are collectively also called "*Fair processing notices*"). Numerous exemptions exist to this rule. However, it is good practice to have some sort of explanation available at the point of collecting the data. The obvious example is to have text added to application forms which briefly explain the processing involved. This can be supplemented by a more detailed statement made available on request. When a form is used to collect personal data, the Information Commissioner recommends that the "*information padlock*" signpost shown on the front of this Note be added to the form, to alert people to the fact that personal data is being collected. It should be noted that as a general rule, your routine use of personal data will be largely restricted to the purposes you describe in the fair processing notice, so it is vitally important to give detailed consideration to the terms of this.
2. Objection to automated processing: you can object to decisions which have a significant effect on you being taken solely by automated means.
3. Objection to direct marketing: you have an absolute right to object to processing for the purposes of direct marketing. In effect the Mail and Telephone Preference Services are put on a statutory footing. On a practical basis, if the Council collects personal data with the intention or expectation that it will send marketing material to that person, they should be told of this up front and given the chance of opting out of the processing.
4. Objection to processing likely to cause distress: the right to object is only if the distress caused by the processing is unwarranted. Proper exercise of Council functions is likely to be unobjectionable.
5. Rights of rectification, erasure and damages: if data are inaccurate you can be forced by a Court to rectify or erase them. In some cases this is limited to the right to post your version of events on the file. If someone suffers damage as a result of a breach of the DPA then they are entitled to compensation for this.

Disclosure to other Council Services

Use of personal data by another Council Service, or for a different purpose within the same service, is subject to the same rules as processing generally. In other words, it must satisfy the *Data Protection Principles*, and you must be able to identify *Schedule 2 condition* (plus a *Schedule 3 condition* for sensitive personal data).

The main difficulty with such “*secondary*” processing is that the fair processing rules require us to have included this within the Article 10 notice. This is done in some circumstances, e.g. benefit applicants and members of staff are advised that their details will be used in fraud detection/income maximisation data matching exercises. In the absence of such notification, data can only be used across departments in limited circumstances, e.g. for purposes of crime prevention/detection or where this is necessary for the purposes of legal proceedings.

Public bodies are often criticised for lack of ‘*joined-up thinking*’ where one department does not pass relevant information to another. Data protection is not a barrier to joined-up thinking; instead, it puts a framework in place which can facilitate this. Possible secondary uses of personal data should be considered and, if this is felt to be worthwhile, use of appropriate Article 10 notices (and perhaps other safeguards) should allow this to happen.

Disclosure to Elected Members

The elected members of the Council, except when meeting in formally constituted Committees, are legally distinct from the Council. Disclosure of personal data to councillors (other than at Committee) therefore counts as disclosure to a third party and accordingly has to be justified in terms of the DP Principles and Schedules 2 and 3. However, the *Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002* modifies the rules in a number of respects. Essentially, if the Council receives a communication from a Councillor or other elected representative (MSP, MP or MEP) acting pursuant to a query which they have received from the data subject, then disclosure of personal data will generally be justified to the extent that it is necessary to respond to the communication.

If the elected representative is acting pursuant to a query from someone other than the data subject, disclosure is only justified: where the data subject cannot consent (e.g. due to mental incapacity); where the Council could not reasonably be expected to seek consent; where seeking consent would prejudice the action the elected representative wants to take; or where disclosure is necessary in the interests of someone other than the data subject but consent has been unreasonably withheld. These rules would apply in cases where the representative acts for the data subject but there is also third party information in the file. Unless these exceptions apply then in general the third party information should not be disclosed.

Disclosure to agents acting on someone’s behalf

It is perfectly competent for someone to appoint an agent to deal with their affairs for them. This can include allowing that other person access to their personal data. If someone claims to be acting on behalf of another person, it is essential to check that the agent has, in fact, been authorised by the individual. Normally this will consist of getting the individual to sign a mandate, but it will still be necessary to check the validity of this (e.g. comparisons with signatures on file, or making contact directly with the individual to confirm matters). Spouses have no particular rights to each other’s details, so this rule should be applied even in cases of married couples or relatives. There is also no exception for solicitors or other professional representatives.

Specific Cases

- CCTV** As noted, images of individuals caught on CCTV can constitute “*personal data*” and should be processed accordingly. The Council has adopted a policy on the Use of CCTV (approved by Policy and Resources on 28 August 2001). All services making use of CCTV equipment must do so in accordance with that policy. The policy can be found on the Financial Services Intranet (Internal Audit/Data Protection).
- Surveillance** This is a situation where Council Services are seeking to obtain information on people deliberately without their knowledge. Covert surveillance is unlawful unless it has been properly authorised in advance by an Investigations Manager. The Council’s Surveillance Policy and supporting documents can also be found on the Financial Services Intranet (Internal Audit/Investigatory Powers).
- Social Work records** These are subject to special rules on subject access. The Council has formulated procedural guidance which explains in detail how this should be handled; this can be found on the Social Work Services intranet under Data Protection.
- Medical Records** If a file contains medical information which came from a health professional rather than from the data subject, special rules apply. These rules are incorporated under the Social Work procedural guidance and reference should be made to this. Someone seeking a copy of their medical records may be charged up to £50 in some circumstances.

Other Legislation

There are a number of other rules concerning the use of personal data and its disclosure. For instance, a number of registers held by the Council must by law be made available to the public. Requests may be made for Committee Minutes and background reports under the Local Government (Access to Information) Act 1985. Environmental Information may have to be disclosed under the *Environmental Information Regulations 1992* (SI 1992/3240). *The Human Rights Act 1998* incorporates the right to respect for private and family life; in deciding whether to disclose personal data it is important to keep this in mind. Lastly, the *Freedom of Information* legislation will mean that all information held by the Council may have to be disclosed to anyone who asks, unless the information is specifically exempt. (Personal data are generally exempt under FOI; other exemptions cover areas such as commercially sensitive information).

Where to get more information

The DPA 98 itself can be accessed at www.legislation.hmso.gov.uk. It is however a very large and impenetrable piece of legislation. Guidance can be found on the Information Commissioner’s web-site at www.dataprotection.gov.uk. This includes specific Codes of Practice on areas such as the use of CCTV and use of personal data in employer/employee relations. General council guidance (including a copy of this guide) can be found on the Financial Services intranet (Internal Audit/Data Protection). Social Work Services’ intranet has detailed guidance material and forms for that Service. Lastly, specific guidance can be obtained from the Council’s Data Protection Officer on 0141 287 7091, from Legal Services on 0141 287 4517, or from individual services’ data protection representatives. A list of these can be found on the Council intranet (Financial Services/Internal Audit/Data Protection/Service Contacts).

Summary

Good practice in data management is likely to satisfy most requirements of DPA 98. In effect, data should only be held which is relevant to the function in question and only utilised for other functions where this can be justified. File management should allow old and unnecessary data to be deleted and subject access requires to be complied with timeously. Again records management systems and archiving arrangements need to be revised to ensure that all records comply with these requirements.

Data protection can be summarised very easily:

NEED TO KNOW

If the information isn't needed or if you don't need to know it, then you probably shouldn't have it or have access to it. Exactly the same rule applies to external parties seeking information from us.

Lastly, the foregoing represents a general summary of the rules and is not a substitute for specific advice. The Data Protection Act is full of quirks and exceptions which may be applicable in the circumstances. Experience has shown that most proposed uses of personal data can proceed with the application of some lateral thinking.

Dr Kenneth Meechan
Assistant Chief Solicitor
Chief Executive's Department
Glasgow City Council

5 August 2003

APPENDIX 1: THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall 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.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area* unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

* *The European Economic Area is the European Union plus Iceland, Norway and Liechtenstein.*

APPENDIX 2: THE “SCHEDULE 2 CONDITIONS”

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.
2. The processing is necessary:
 - a) for the performance of a contract to which the data subject is a party; or
 - b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller 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:
 - a) for the administration of justice;
 - b) for the exercise of any functions conferred on any person by or under any enactment;
 - c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or
 - d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6.
 - i. for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data is 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.
 - ii. the First Minister may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

APPENDIX 3: THE “SCHEDULE 3 CONDITIONS”

CONDITIONS RELEVANT FOR THE PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.
2.
 - a) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
 - b) The First Minister may by order:
 - i. exclude the application of sub-paragraph a) above in such cases as may be specified; or
 - ii. provide that, in such cases as may be specified, the condition in sub-paragraph a) above is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary:
 - a) in order to protect the vital interests of the data subject or another person, in a case where:
 - i. consent cannot be given by or on behalf of the data subject; or
 - ii. 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 carried out in the course of its legitimate activities by any body or association which:
 - i. is not established or conducted for profit; and
 - ii. exists for political, philosophical, religious or trade-union purposes,
 - b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
 - c) relates only to individuals who either are members of the body or association or have regular contract with it in connection with its purposes; and
 - d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing:
 - a) is necessary for the purpose of, or in connection with, any legal proceedings (including 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.
7. a) The processing is necessary:
 - i. for the administration of justice;
 - ii. for the exercise of any functions conferred on any person by or under an enactment; or
 - iii. for the exercise of any functions of the Crown, a Minister of the Crown or a government department.b) The First Minister may by order:
 - i. exclude the application of sub-paragraph a) in such cases as may be specified; or
 - ii. provide that, in such cases as may be specified, the condition in sub-paragraph a) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
8. a) The processing is necessary for medical purposes and is undertaken by:
 - i. a health professional; or
 - ii. 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.b) In this paragraph "*medical purposes*" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
9. a) The processing:
 - i. is of sensitive personal data consisting of information as to racial or ethnic origin;
 - ii. 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; and
 - iii. is carried out with appropriate safeguards for the rights and freedoms of data subjects.b) The First Minister may by order specify circumstances in which processing falling within sub-paragraph a) i. and ii. is, or is not, to be taken for the purposes of sub-paragraph a) iii. to be carried out with appropriate safeguards for the rights and freedoms of data subjects.
10. The personal data are processed in circumstances specified in an order made by the First Minister for the purposes of this paragraph.

Two orders have been made under this provision: the Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417) which covers criminal investigation, confidential counselling services, etc. and the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 (SI 2002/2905) referred to in the "*elected members*" note.



GLASGOW CITY COUNCIL CRIMINAL INVESTIGATION RELEASE FORM

For releasing Personal Data to Police/
HM Revenue and Customs/Benefits
Agency

Please complete all sections in BLOCK CAPITALS

REQUESTING OFFICER: Rank _____ Name _____

FORCE AND DIVISION: _____ Badge No _____

Contact Address _____

Phone _____ Fax _____

I, [Name] _____ hereby request the following information from Glasgow City Council: [insert details of information requested]

I hereby confirm that the above information is required for one or more of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of any tax or duty or of any imposition of a similar nature

and that this purpose/these purposes would be prejudiced if Glasgow City Council do not release the information as requested.

The disclosure of this information is proportionate to what is sought to be achieved with it. I further confirm that in terms of Section 29(1) of the Data Protection Act 1998, it would prejudice this investigation if the data subject(s) described above is/are notified of this disclosure.

I understand that the information is being released to me purely for the above purpose(s) and I undertake not to use the information for any other purpose (including 'use' consisting of disclosure to outside agencies). The information disclosed shall only be retained beyond the timescales required for any present investigation where such retention is in compliance with all applicable laws relating to the retention of criminal intelligence.

Signature of applicant _____ Date _____

AUTHORISING OFFICER'S STATEMENT - must be completed by the following rank or above (for urgent requests only, the lower rank in brackets may authorise): Police: Chief Inspector (Inspector); Customs: Band 8 (Band 7); Inland Revenue: Band C1(C2); Benefits Agency: Band C4 (C3).

I, [Print name and rank] _____ hereby authorise the above request for information.

Signature of A/O _____ Date _____

NOTE FOR GLASGOW CITY COUNCIL STAFF: This form has been prepared by Legal Services. If properly completed, it allows the Council to release information to the investigating agency in terms of the Data Protection Act 1998 Section 29 and additionally exempts the Council from notifying the individuals whose details are released that this disclosure is being made. Please note that it is still necessary to check the identity of the requesting officer. A copy of the completed form must be kept on file.

The Data Protection Act 1998 Section 29(1) – Personal data processed for any of the following purposes – (a) the prevention or detection of crime, (b) the apprehension or prosecution of offenders, or (c) the assessment or collection of any tax or duty or of any imposition of a similar nature, are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3 and section 7 in any cast to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.