NATIONAL LIBRARY OF SCOTLAND

DATA PROTECTION POLICY

APPROVED BY: SMT (26 June 2008)
LLT (26 January 2016) (Revised)

REASON FOR POLICY: It is vital that all staff and all contractors, consultants, volunteers and others are fully aware of their responsibilities for the proper processing of personal data as required by the Data Protection Act 1998. This policy identifies the responsibilities that staff have to ensure the Library's compliance with this legislation. It is accompanied by a series of appendices designed to help understand certain complex areas connected with the processing of personal data.

SCOPE: This policy applies to all National Library of Scotland employees, to members of the Board and to others carrying out work for the Library including contractors, consultants, volunteers and any other such agents.

CONTACT: If you are uncertain about any aspect of this policy or require further information contact the Intellectual Property Specialist.

Section		Page
POLICY		3
APPENDIX I	Definitions within the Data Protection Act 1998	18
APPENDIX II	The eight data protection principles	20
APPENDIX III	Rights of data subjects	22
APPENDIX IV	Capturing personal data	25
APPENDIX V	Processing personal data	27
APPENDIX VI	Third party personal data in the Library collections	30
APPENDIX VII	Personal data that the Library doesn't "own"	32
APPENDIX VIII	Holding of publishers' details	33
APPENDIX IX	Names of donors in fundraising campaigns	35

POLICY

1. Status of the Policy

1.1. Compliance with this policy is a requirement for employees and members of the Board of the National Library of Scotland (the Library); it is also a requirement for others carrying out work for the Library, including contractors, agency staff, placement students and volunteers.

1.2. The policy reflects the duties that the Library must perform under the Data Protection Act 1998 (the Act) and best practice guidance. The policy explains the responsibilities of staff and is accompanied by guidance notes.

1.3. Compliance with the Act is the responsibility of all members of staff of the Library. A breach of the terms of this policy, whether deliberate or through negligence, could lead to disciplinary action. A breach of the Act may also lead to legal or regulatory proceedings. Staff should note that unauthorised disclosure of personal data may be a disciplinary matter, and could be considered gross misconduct in certain cases.

1.4. Researchers using Library collections must also comply with the Act, and separate guidance will be issued for readers and researchers.

2. The Data Protection Act 1998

2.1. The Act covers the personal data of identifiable living individuals and replaced Data Protection Act 1984. The Act distinguishes between ordinary personal data such as name, address and telephone number, and sensitive personal data relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive data is subject to stricter conditions. In particular, processing of sensitive data requires explicit consent. While the Act permits the processing of data without consent where this is for the legitimate activities of an institution and is not to the detriment of individuals, in most instances consent to process ordinary and sensitive data is obtained routinely by the Library for the avoidance of doubt.

3. Definition of personal data

3.1. The Act covers all personal data processed by the Library, irrespective of where this is held, including, but not limited to data held by individual members of staff in their own files, data held in departmental or centralised filing systems and personal data held in Library collections.

The Freedom of Information (Scotland) Act 2002 (FOISA) extended the scope of the Act to include “category (e) data”, which means in practice

that all personal data held by the Library is covered by the Act. Further information regarding the definition of personal data is given in Appendix I.

4. Responsibilities

4.1. The Library and its staff must process personal data in accordance with the Data Protection Act. The Act contains eight data protection principles (prescribed in Schedule 1 of the Act – further information about the eight principles is given in Appendix II). The data protection principles detail that the main responsibilities for all staff are:

i. Personal data must be processed fairly and lawfully and shall not be processed unless certain conditions are met (see Appendix II).

ii. Personal data shall only be processed for the purpose or purposes for which it has been gathered.

iii. Personal data must be adequate, relevant and not excessive for those purposes.

iv. Personal data must be accurate and kept up to date.

v. Personal data must not be kept for longer than is necessary for that purpose.

vi. Personal data must be processed in accordance with the data subject's rights.

vii. Personal data must be kept safe from unauthorised access, accidental loss or destruction.

viii. Personal data must not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

4.2. The Library is the Data Controller under the Act, and as such its senior management are ultimately responsible for ensuring compliance. The Library's senior management regard the lawful and correct treatment of personal information as of vital importance to successful business operations, and to maintaining confidence with whom we deal.

4.3. The Intellectual Property Specialist is responsible for keeping the Library's notification with the Information Commissioner up to date. The Intellectual Property Specialist is also responsible for assisting all members of staff in complying with their obligations under this policy, and for issuing guidance and training.

4.4. The Intellectual Property Specialist is responsible for managing Subject Access Requests (SARs) received by the Library.

4.5. Heads of Department have day-to-day responsibility for ensuring compliance with the Act. They are responsible for ensuring that their staff are made aware of the existence and content of this policy, and that the personal data held by their department is kept securely and used properly, within the terms of the Act. They are also responsible for informing the Intellectual Property Specialist of the types of personal data held in their divisions, and any changes to, or new holdings of, personal data, either within business information or Library collections.

4.6. Line Managers are responsible for ensuring that staff who have specific data protection responsibilities have these written into their job descriptions and forward job plans, and for ensuring that staff receive the training necessary to fulfil their responsibilities under this policy. Line Managers are also responsible for auditing compliance with the retention schedules with the Intellectual Property Specialist.

4.7. All members of staff who create, receive or otherwise process personal data have responsibilities under the Act. Staff must ensure that any request for personal data they receive is handled in compliance with this policy (see section 8). Specifically, members of staff are responsible for:

4.7.1. familiarising themselves with this policy and the accompanying guidelines;

4.7.2. familiarising themselves with the implications of data protection in their job;

4.7.3. seeking advice from the Intellectual Property Specialist when uncertain about the appropriate action to take with respect to the processing of personal data – particularly when sensitive personal data is involved;

4.7.4. managing documents and records in accordance with this policy and the Records Management Policy;

4.7.5. ensuring that any personal data they hold is held securely, that it is accurate and up to date, and that any personal data they hold is not passed to any unauthorised third party.

5. Data Security

5.1. All employees, members of the Board and others carrying out work for the Library including contractors, consultants, volunteers and any other such agents must comply with the terms of the Information Security Policy.

5.2. Staff should make reasonable efforts to ensure that all personal information is kept securely, with particular attention to the security of sensitive data. Personal data should be kept in a lockable room with

controlled access, kept in a locked filing cabinet or drawer, or protected by password, if held on a computer.

5.3. The Scottish Government requires all users of laptops, mobile phones and other portable equipment to protect the devices by password or PIN. Detailed guidance on how to do this is available from the ICT Helpdesk. Users of portable ICT and removable media devices are reminded are responsible for the security of the data held on these devices when they are working off site and should not leave devices unattended. Information Systems staff will provide software to encrypt data on all laptops, removable media and storage devices such as USB / flash drives to meet the Scottish Government's requirements. It is strongly recommended that sensitive information not be stored on portable media, taken off-site or stored on non- Library equipment.

5.4. Heads of Department are responsible for ensuring appropriate technical and organisational measures are taken within divisions to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, such data.

5.5. All staff must ensure casual access to personal data is not possible, for example by members of the general public seeing VDU screens or printouts. VDU screens should be cleared after use, and terminals should not be left unattended without being locked or shut down. Printouts should be kept securely, and disposed of in a confidential manner when no longer required. Particular care must be taken when portable devices are used in public places, on public transport or when working at home.

5.6. Secure networks must be used where available. Personal data sent via non-secure networks are to be encrypted. When sending sensitive data on portable media (e.g. USB memory sticks), the portable media must be password protected and the data encrypted; the data should be sent via a secure posting method such as special delivery.

5.7. Data transfer agreements between the Library and other organisations are to be given formal approval by the Intellectual Property Specialist.

6. Collecting personal data

6.1. Whenever it is reasonable to do so, and when the Library's functions and obligations do not require it, personal data should not be collected.

6.2. Statements on data capture forms should be as explicit as possible and state precisely the purpose(s) for which the data are being collected, the recipients of that data, the manner in which it will be stored, and how long it will be kept for(see Appendix IV).

6.3. All personal data capture forms must be submitted for approval by the Intellectual Property Specialist.

7. Consent for processing

7.1. Wherever possible, personal or sensitive data should not be obtained, held, used or disclosed unless the data subject has given consent. "Consent" means that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information is not valid. There must be active communication between the parties, such as a form signed freely of the data subject's own accord. Silence does not equal consent and consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of the data subject must be obtained unless the data subject's vital interests (life and death) are at stake. Consent to process data held in Library collections is considered separately in section 9 of this policy.

7.2. In most instances consent to process personal and sensitive data is obtained routinely by the Library (e.g. when a reader signs a registration form or when a new member of staff signs a contract of employment). Any Library forms (whether paper-based or web-based) that gather data on an individual must contain a statement explaining what the data will be used for and to whom it may be disclosed.

7.3. If an individual does not consent to certain types of processing (e.g. direct marketing), then that processing may not take place. Data processors must mark the records appropriately to record that the data subject does not wish their data to be processed for that particular purpose.

7.4. Whenever there might be a conflict between the legitimate interests of the Library and the rights, freedoms and legitimate interests of the data subject, the member of staff who is processing the data will contact the data subject to elicit clarity on the issue. This may typically be to seek permission for the further processing of personal data.

7.5. To pursue the Library's legitimate interests with regard to fundraising, the Library's Development staff need to do a certain amount of background research and profile building in order to evaluate prospective donors for contact. Guidance on this is given by the Institute of Fundraising and the Library has based this part of the policy on that guidance. Provided that the data is not sensitive, but freely available and in the public domain, staff will not be found to be processing data unfairly or unlawfully in the compilation of prospective donor files, provided that at the first point of contact with such a donor, an appropriate declaration is made regarding the holding and processing of that person's data. (See Appendix IX)

7.6. The second principle of the Act stipulates that personal data obtained for one or more specified and lawful purposes should not be further processed in any manner incompatible with that purpose or those

purposes. However, personal data can be further processed providing that the processing is fair and lawful and meets the necessary requirements as listed in schedule 2 and / or 3. In other words, personal data can be processed further if the data subject gives their permission. All staff who wish to process personal data for purposes other than the original purpose for which it was collected must use the flowchart in Appendix V to determine whether this further processing is lawful.

8. Right of access to personal data

8.1. The Act grants several rights to data subjects (see Appendix III). The key right is the right to make a request for access to your own personal data. This is called a Subject Access Request (SAR). In the event of receiving a SAR, the following steps should be taken:

8.1.1. Request proof of identification to ensure the applicant is the data subject. Personal data must not be disclosed to anyone other than the data subject (unless the request is a section 29 request from the police – see 8.3). You do not need to request proof of identification if the identity of the applicant is known to you, for example because they have already provided evidence or they are known to you personally.

8.1.2. Record the date the request was received. The Library has 40 calendar days to fulfil a subject access request.

8.1.3. Notify the Intellectual Property Specialist as soon as possible.

8.1.4. Inform the applicant that the Library reserves to right to charge the prescribed maximum fee (currently £10) for the satisfaction of a subject access request. In the event of recovering category (e) personal data, the Library may charge for recovery of information up to maximum amount prescribed (currently £50) and may refuse a request where the cost of compliance would exceed the prescribed amount, which is currently £600.

8.2. Requests for another person's personal data are to be handled under FOISA. There are exemptions within FOISA which cover access to the personal data of others. It is unlikely that another person's personal data would be released as a result of a FOISA request. .

8.3. There is a notable exemption within the Data Protection Act which allows personal data to be disclosed to the police in order to support the prevention or detection of a crime. Personal data should only be considered for disclosure to the police upon the receipt of a written request for access under section 29 of the Act. Staff should direct any such requests to the Intellectual Property Specialist.

9. Use of personal data in Library collections for research purposes

9.1. Personal data held within the Library's collections is also subject to the Act. This section applies especially, but not exclusively, to personal data held in manuscript and moving image collections.

9.2. Section 33 of the Act exempts personal data from the coverage of the Act when, and only when, it is used for the purposes of research, and furthermore, only when the relevant conditions are met. The relevant conditions are that:

9.2.1. the data is not processed to support measures or decisions with respect to particular individuals;

9.2.2. the data is not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject;

9.2.3. the results of the research or any resulting statistics are not made available in a form which identifies data subjects.

9.3. Whenever personal data held in the Library's collections is used, researchers and staff must abide by the conditions set out in section 9.2 above. All users when signing the Reader's Registration Form agree to section 1 of the code of practice, which says that "Readers should ensure that any information obtained from our collections relating to living individuals is used in accordance with the principles of the Data Protection Act 1998". Where the personal data appears in a journal or monograph that has been published, it is assumed that the publisher takes on board the liability for any damage or distress that may be caused to data subjects as a result of their personal data being made known in the initial circumstance, that being the publishing of the material in the first place. The Library will not be in breach of the Act by making already published material available.

9.4. Release of unpublished personal data in Library collections must be handled as if the Library were the publisher with related liabilities.

9.5. Identifying personal data in Library collections is difficult. Since the Act only applies to living individuals, and since it cannot readily be known whether an individual is still alive, a life expectancy of 100 years is to be assumed.

9.6. In order to enable the best practice in this area and to prioritise resources, staff must identify collections that fit one or more of the following criteria:

9.6.1. Sensitive personal data of identifiable living individuals is known to be within the collections, and this sensitive personal data is unlikely to already be in the public domain.

9.6.2. A data subject has noted that they think their sensitive personal data may be part of a particular collection.

9.7. Notwithstanding the above, staff working with the collections may be able to make a more informed judgement about the sensitivity of data contained in the collections based upon:

9.7.1. Whether the sensitive personal data is already publicly known (for example it would probably not be sensible to treat as sensitive the fact that a well-known leader of a trade union was a member of a trade union);

9.7.2. Whether staff had learned through their dealings with donors, depositors, vendors and such like that there were issues of sensitivity surrounding the collection;

9.7.3. Their own curatorial knowledge of the collections.

9.8. Catalogues and inventories should note the presence of sensitive personal data, and collection boxes should be marked in a clear way to identify the presence of personal data.

9.9. When a collection contains sensitive personal data, the curator in charge of the collection should consider restricting access to the collection until such time that the sensitivity of the personal data ceases to be an issue.

9.10. In the event that a researcher requests access to a collection that has been identified as containing sensitive personal data, the curator in charge of the collection must consider whether granting access to the material would constitute fair processing. The Library received guidance from the Information Commissioner in response to a case that it submitted regarding the rights of a third party data subject in a manuscript collection (see Appendix VI). Based on the conclusions of the Information Commissioner's investigation, a curator in charge of a collection should now consider contacting the third party data subject(s) to request their permission to process their personal data. The decision to contact the data subjects should be based on the following criteria:

9.10.1. Whether they are living, identifiable individuals.

9.10.2. How much work would be involved in contacting the data subject or establishing whether they were still alive.

9.10.3. How much distress or damage is likely to be caused to the data subject by allowing access to their personal data for research purposes.

The Information Commissioner's response indicated that the Library would not be in breach of the researcher's rights under section 33 by forbidding access to manuscript and moving image collections when it was protecting the rights of third party data subjects.

9.11. Consent to process personal data may only be given by the data subject. Consent cannot be given by a collection owner, or by another data subject within the collection.

9.12. In the event that the curator wishes to process the personal data of the third party data subject without seeking their consent:

9.12.1. the curator must assess the risks to the Library and report this assessment to the Library Leadership Team;

9.12.2. the researcher remains bound by the terms of section 33 of the Data Protection Act (see paragraph 9.2).

The Library may receive a complaint from the data subject and would need to be able to explain its decision to the data subject and to the Information Commissioner, who may undertake to investigate the data subject's complaint.

9.13. Curators must ensure that all Library users consulting collections where the personal data of living individuals is likely to be present must sign the declaration form "Permission to consult material which may contain personal data as defined by the DPA 1998". A new form should be signed for each collection of material that is likely to feature personal data about living individuals.

9.14. The Information Commissioner's investigation into the case submitted by the Library confirmed that managing data protection compliance was compromised when the identity of the data controller was in doubt. This was mainly an issue where collections had been purchased with access permission conditions attached. Because the Commissioner responded in favour of the third party data subject, this means that irrespective of any arrangement made during the acquisition process, the Library must endeavour to uphold the rights of the data subject, which will typically involve seeking their consent to process their personal data. Furthermore:

9.14.1. In the event of the data subject refusing to consent to access to their personal data when it has been sought by the Library, no access can be given. In the event of a FOISA request it would be appropriate to cite section 38 as the reason for withholding data.

9.14.2. The third party data subject may stop the disclosure of their data, but they may not ask for its destruction. If they believe that there are inaccuracies in their personal data within Library collections, a note should be appended to the original item to that effect. This will allow the integrity of the historical record to remain intact whilst at the same time recording the data subject's correction.

9.15. The Library acquired many of its collections prior to this legislation, and some of the clauses in the terms of purchase or acquisition have

bound the Library to consult with the original collection owner or equivalent with regard to access. This has made the management of access and data subject rights problematic. The Library's policy now is that:

9.15.1. Any new collections should not be bought with access restrictions in place. During negotiations, the Library's duties under the Act and the FOISA should be explained, and the Library should become the sole data controller of the material that owns. Curators should seek advice from the Intellectual Property Specialist as needed.

9.15.2. Following the Commissioner's conclusions, the Library understands that it is allowed to take the final decision to withhold access to personal data in collections either upon request by a data subject who would suffer substantial distress or damage, or based on its own assessment in its role as data controller, irrespective of any contractual ambiguity regarding access permissions. This applies when the material in question is owned by the Library. Where possible, old agreements should be reworked to fit the standard described in 9.11.1.

9.16. When material is deposited with us, the depositor must be made aware that they remain the data controller and must also be made aware of their responsibilities under the Act. Curators involved in arranging deposit agreements for collections containing unpublished personal data (typically but not exclusively manuscript and moving image collections) must contact the Intellectual Property Specialist to discuss the terms of the agreement before it has been signed.

10. CCTV footage

The use of closed circuit television cameras (CCTV) by the Library on its premises is covered by the Act. The Information Commissioner has produced a Code of Practice (20015) which stipulates what organisations are required to do to comply with the legislation. All staff must abide by the Code of Practice, and failure to do so may result in disciplinary action. The Code of Practice does not cover the use of conventional cameras on Library premises; it only covers the images that are captured via CCTV. Copies of the full Code of Practice can be downloaded from https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf. The rest of section 10 refers to key elements of the Code of Practice and states who is responsible at the Library for compliance.

10.1. The Library has approximately 150 overtly placed CCTV cameras on its premises. There are no covert cameras sited at any of the premises of the Library. The use of any such cameras, if required, will be exceptional, limited and within the requirements of the Code of Practice and other relevant legislation in any of our premises.

10.2. The Security and Cleaning Services Manager has overall responsibility for managing the Library's CCTV scheme. The Security and Cleaning Services Manager is the operational manager of the cameras.

10.3. The operational manager is responsible for:

10.3.1. handling any faults with the CCTV machinery;

10.3.2. ensuring that CCTV signs and awareness is adequate and effective;

10.3.3. ensuring that all staff with access to CCTV machinery use it appropriately and in line with the Code of Practice. .

10.4. All staff who use CCTV machinery or who have access to it must abide by the Code of Practice, and failure to do so may result in disciplinary action. Specifically:

10.4.1. Staff must only operate CCTV cameras for the purposes of the prevention and detection of crime and for the purposes of public safety and wellbeing;

10.4.2. Staff must make sure that there is no unauthorised access to the CCTV system or the CCTV control room;

10.4.3. Staff must ensure that CCTV cameras are not used to look into private residential properties.

10.5. Disclosure of CCTV images should only be to law enforcement agencies, or to a data subject in response to a subject access request. The process for handling a subject access request or a request for access from the police is just the same as in section 8 above. Data subjects who request access must provide details which allow the Library to identify them as the subject of the images and also to locate the images on the system. If images of third parties are also shown with the images of the person who has made the access request, the Intellectual Property Specialist and the Security and Cleaning Services Manager must consider whether the images of third parties should be obscured. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured. In many cases, images can be disclosed as there will not be such intrusion. The Information Commissioner cites these examples:

- *A public space CCTV camera records people walking down the street and going about their ordinary business. Where nothing untoward has occurred, this can be released without editing out third party images.*

- *Images show the individual who has made the request with a group of friends, waving at a camera in the town centre. There is little expectation of privacy and the person making the request already knows their friends were there. It is likely to be fair to release the image to the requester without editing out the faces of their friends.*

- *Images show a waiting room in a doctor's surgery. Individuals have a high expectation of privacy and confidentiality. Images of third parties should be redacted (blurred or removed) before release.*

10.6. The Act does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. The Code of Practice states that retention should reflect an organisation's own purposes for recording images, and that images should not be kept for longer than strictly necessary to meet your own purposes for recording them. Images may need to be retained for a longer period, where a law enforcement body is investigating a crime, to give them opportunity to view the images as part of an active investigation. The Library's CCTV images are stored digitally and are retained for a period of 30 days, after which they are overwritten. The Security and Cleaning Services Manager is responsible for ensuring compliance with the retention and disposal of CCTV images.

11. Other legislation and statutory requirements to consider

11.1. The Human Rights Act 1998, Schedule 1, Part 1, Article 8 (Right to Respect for Private and Family Life) is particularly worth considering with regard to the processing of personal data. The Library must ensure that any processing of personal data is fair and legitimate, and does not violate this human right.

11.2. The common law of confidence protects information and personal data provided that it can be shown that:

- the information in question has the necessary 'quality of confidence'. This means that the information should not be in the public domain or readily available from another source (though the fact that the information may be known to a limited class of persons does not destroy confidentiality) and it should have a degree of sensitivity and value;

- the information in question was communicated in circumstances giving rise to an obligation of confidence. The obligation of confidence may be express or implied from the circumstances;

- there was an unauthorised use of that material.

Private and personal correspondence between two people would likely qualify as having the necessary quality of confidence. An email sent to a number of people about a non-confidential work related matter would probably not qualify as having the necessary quality of confidence. When considering whether the processing of personal data would be fair and lawful, consideration must be given to the common law of confidence. Personal data should not be processed if to do so would breach the common law.

11.3. Section 68 of the Freedom of Information Act 2000 (the legislation covering England and Wales) amended the Act to extend the definition of the word "data" to include "recorded information held by a public authority [that] does not fall within any of paragraphs (a) to (d)". Statutory Instrument 2004 No. 3089 (S.10) applied this extended definition in Scotland.

11.3.1. The effect of this was to create a new category, category (e) data, which means that all data held by a public authority, paper or electronic, in a filing system or not, is covered by the Act. Category (e) data is data which is manual (paper) and not held in a relevant filing system (i.e. not filed and indexed in a way that would enable the data to be readily found with little knowledge of the files themselves).

11.3.2. However, category (e) data is exempt from the first, second, third, fifth, seventh and eight principles, and also from sections 10, 11 and 12. There are other partial exemptions from section 13 and from the sixth principle. In other words, the Act only applies to category (e) personal data insofar as the data subject may request access to this data and exercise their right to stop the processing of it or to amend inaccuracies.

11.3.3. This right of access is dependent on the data subject's ability to describe what data it is that they are seeking, and where it might be. The Library is not obliged to retrieve category (e) data if the data subject cannot describe what it is that they are looking for. Furthermore, if the cost of recovering the data would exceed the prescribed amount, a public authority is not obliged to undertake the task. The charging structure used to determine FOISA charges is to be used to calculate any such costs.

11.3.4. The right of access under FOISA and the "right to privacy" suggested by the Act may appear to be at odds with each other. However, section 38 of FOISA clarifies this. Personal data is exempt from FOISA where the request is for a data subject's own data. If a person requests their own data they are making a SAR under the Act and not a request under FOISA. Note that there are different requirements for handling a FOISA request and a SAR, for example the time allowed for issuing a response.

11.3.5. FOISA allows people to request access to other people's personal data. However, this data can only be released if this would not constitute unlawful or unfair processing, or breach any of the data protection principles, or would not cause damage or distress. In practical terms it would be difficult to envisage releasing one person's personal data to a third party without breaking most or all of these conditions. Unless personal data is in some way already in the public domain, it would be reasonable to assume that personal data would not be released as a result of a FOISA request.

12. Retention and disposal of personal data

12.1. The fifth data protection principle states that "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes". Keeping data indefinitely, or for arbitrary periods without any justifiable reason not only breaches this principle, but also makes it more likely that other principles will be breached. The likelihood of personal data changing increases over time. Therefore, the longer the retention of personal data, the more likely it is that the fourth principle will be breached ("Personal data shall be accurate and, where necessary, kept up to date").

12.2. It is not in the interest either of data subjects or of the Library to retain unnecessary or duplicate information. The Library does retain some data in order to comply with statutory requirements. The following factors are likely to impact on how long the Library retains personal data:

12.2.1. The personal data is still serving the purpose for which it was acquired.

12.2.2. There is a legal responsibility to retain the personal data for a particular length of time.

12.2.3. Retention is necessary for the purposes of legitimate interests pursued by the data controller and the processing does not conflict with the rights and freedoms or legitimate interests of the data subject.

A retention period should take into consideration all of these issues, but should not be excessive in response to 12.2.3.

12.3. Retention of information, including personal data, is governed by the Records Management Policy and the Business Classification and Retention Scheme.

13. Review

13.1. This policy will be reviewed every two years or sooner as required, for example due to regulatory change.

13.2. The Intellectual Property Specialist has responsibility for overseeing review of this policy. Any changes to this policy are to be approved by the Library Leadership Team.

APPENDIX I – Definitions within the Data Protection Act 1998

These are the terms as they are defined in the Act:

"**Data**" means information which-

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d);

"**Data controller**" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed;

"**Data processor**", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

"**Data subject**" means an individual who is the subject of personal data;

"**Personal data**" means data which relate to a living individual who can be identified-

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

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

"**Processing**", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data;

"**Relevant filing system**" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by

reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

"Sensitive personal data" means personal data consisting of information as to the racial or ethnic origin of the data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

"Special purposes" means processing personal data with a view to the publication by any person of any journalistic, literary or artistic material, or for research (statistical and historical) purposes.

APPENDIX II – The eight data protection principles

The Data Protection Act derives most of its substance from the eight data protection principles in Schedule 1 of the Act. Of the eight principles, the most important is the first. This in turn derives most of its substance from Schedules 2 and 3.

The interpretation of these principles will be made clearer in the next section of this document, which deals with the Library's processing of personal data. The main issue to bear in mind at the moment is the importance of the first principle, and the specific conditions that must be met in order for data processing to be considered fair and lawful.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

at least one of the following conditions is met:

1. The data subject has consented to the processing of their data;
2. The processing is necessary
   a) for the performance of a contract to which that 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;
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
   d) for the exercise of any other functions of a public nature exercised in the public interest by any person;
6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Note – the above conditions form Schedule 2 of the Act and relate to the fair and lawful processing of non-sensitive personal data. In the

interests of brevity, Schedule 3 conditions for the processing of sensitive personal data are not included here. As may be expected, the conditions are even more stringent.

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.**

In addition to the 28 EU member states and Iceland, Liechtenstein, and Norway (together the European Economic Area, EEA), the European Commission has recognised the following as providing adequate protection for personal data processing; Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, and the United States Bureau of Customs and Border Protection (transfer of air passenger name records). This list is not static. For the latest, visit: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

APPENDIX III – Rights of data subjects

In addition to the obligations placed upon data controllers, the Act also grants a number of rights to data subjects. These rights include the right to request access to all personal data held about them by a data controller, and the right to prevent processing by a data controller. The rights of data subjects are detailed in the following extracts from the Act:

Section 7 (Right of access to personal data)

(1) An individual is entitled:

a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller;

b) if that is the case, to be given by the data controller a description of-
   i. the personal data of which that individual is the data subject,
   ii. the purposes for which they are being or are to be processed, and
   iii. the recipients or classes of recipients to whom they are or may be disclosed;

c) to have communicated to him in an intelligible form-
   i. the information constituting any personal data of which that individual is the data subject, and
   ii. any information available to the data controller as to the source of those data; and

d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.

(2) A data controller is not obliged to supply any information under subsection (1) unless he has received-

a) a request in writing, and

b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

(3) A data controller is not obliged to comply with a request under this section unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which that person seeks.

(4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless-

a) the other individual has consented to the disclosure of the information to the person making the request, or

b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual

…

(6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to-

a) any duty of confidentiality owed to the other individual,
b) any steps taken by the data controller with a view to seeking the consent of the other individual,
c) whether the other individual is capable of giving consent, and
d) any express refusal of consent by the other individual.

Section 10 (Right to prevent processing likely to cause damage or distress)

An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the ground that, for specified reasons-

a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another, and
b) that damage or distress is or would be unwarranted.

Section 11 (Right to prevent processing for the purposes of direct marketing)

(1) An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject.

(2) If the court is satisfied, on the application of any person who has given a notice under subsection (1), that the data controller has failed to comply with the notice, the court may order him to take such steps for complying with the notice as the court thinks fit.

(3) In this section "direct marketing" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

Section 12 (Rights in relation to automated decision taking)

(1) An individual is entitled at any time, by notice in writing to any data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data in respect of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct.

(2) Where, in a case where no notice under subsection (1) has effect, a decision which significantly affects an individual is based solely on such processing as is mentioned in subsection (1)-

a) the data controller must as soon as reasonably practicable notify the individual that the decision was taken on that basis, and
b) the individual is entitled, within twenty-one days of receiving that notification from the data controller, by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.

Section 13 (Right to compensation)

(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if-

a) the individual also suffers damage by reason of the contravention, or
b) the contravention relates to the processing of personal data for the special purposes.

(3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.

Section 14 (Rectification, blocking, erasure and destruction)

If a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contain an expression of opinion which appears to the court to be based on the inaccurate data.

APPENDIX IV – Capturing personal data

Data protection compliance begins with the data capture process. The Library has a very broad range of purposes registered with the UK Information Commissioner. These purposes notify the Commissioner of the possible scenarios in which the Library may process personal data, but they do not automatically mean that personal data can be processed. It is the satisfaction of the first data protection principle that legitimises the processing of personal data.

The first principle depends largely on receiving the consent of the data subject to process their data. The more explicit the contract between data subject and data controller, the more likely it is that data subjects can correctly give or decline their consent. When the terms of the contract are implicit, it is not enough to assume that the data subject will have the same understanding as the data controller. If the data subject feels that the nature of the processing of their data was not correctly implied, they may have a reasonable case to bring to the Information Commissioner for unfair processing. For the avoidance of any doubt, explicit contracts should be written wherever possible.

Really good data protection compliance begins before personal data is even acquired by asking "What data do we want, and why do we want it?" It may be that in order to fulfil a business function or objective, the Library does not even need to acquire personal data, or can capture the data anonymously. The result is simple – if the Library does not hold personal data, it does not have to manage it according to the Act.

It is at the point of data capture that the "contract" between the data subject and the data controller is formed. This contract can be of two types: the explicit contract and the implicit contract.

The explicit contract is formed when the data controller states that they are the data controller, and that they will use the personal data for a specific named purpose or purposes, and will process the data in a certain way. The data subject is asked to sign an agreement that they give their consent to this processing.

Note, however, that an implicit contract can exist when there is no signed agreement, but when there is a realistic expectation that personal data will be processed only in a certain way or to a certain extent. When this type of contract exists the common law of confidentiality must be considered, and processing should not take place if such processing would run contrary to the common law (see section 10.2 of the policy).

With specific regard to collections the Library can find itself in situations where it becomes the holder of personal data that has been acquired without the knowledge or consent of the data subject. A ruling by the Information Commissioner implies that the rights of data subjects should be upheld in

these circumstances, although this ruling is complex. The complexities are further explained in Appendix VI.

Irrespective of the way in which data has been captured, it is the responsibility of the Library to ensure that all data is collected and processed in accordance with the Data Protection Act, the common law of confidentiality, the Human Rights Act, and other statutory obligations.

APPENDIX V – Processing personal data

It is important to note that under the Act, simply holding personal data is classed as processing personal data. Processing includes the following: obtaining, recording, holding, using, organising, adapting, altering, retrieving, consulting, transmitting, disclosing, erasing, destroying, and combining. Whenever any of these activities occur with regard to personal data, the Library must ensure that these activities uphold the data protection principles. On a day to day basis, this should mean doing the following:

Security

- Staff working in public areas should ensure that there are no personal data files and folders within access to members of the public. Folders documenting accidents or incidents should be kept in offices rather than at the issue desks.
- Elsewhere, cupboards and filing cabinets that contain sensitive personal information should be kept locked. Sensitive personal data relating to staff should be held within the Human Resources department.
- Increasingly, personal data is stored on computers. All computers must be "locked" when not in use.
- Do not fulfil a Subject Access Request unless the identity of the applicant has been confirmed. Do not give out personal data to anyone other than the data subject.
- Requests for access to personal data from the Police must be made in writing to the Intellectual Property Specialist.

Data integrity

It is important to update records of personal data. Incorrect names and addresses can result in sending out correspondence to a deceased person or to the home of a person who has divorced from their spouse. It is not always possible to hold personal data in one system, but every effort should be made to keep address lists and other repositories of personal data to a minimum. Ensure that all related records are updated when personal details change. Destruction of personal data once it has served its purpose (and satisfied any statutory requirements) is a good way to minimise the risk of inaccurate data holdings. Destruction of personal data should correspond to the Records Management Policy.

Use of data

The second principle requires data controllers to obtain personal data only for one or more specified and lawful purposes, and not to further process personal data in any manner incompatible with that purpose or those purposes

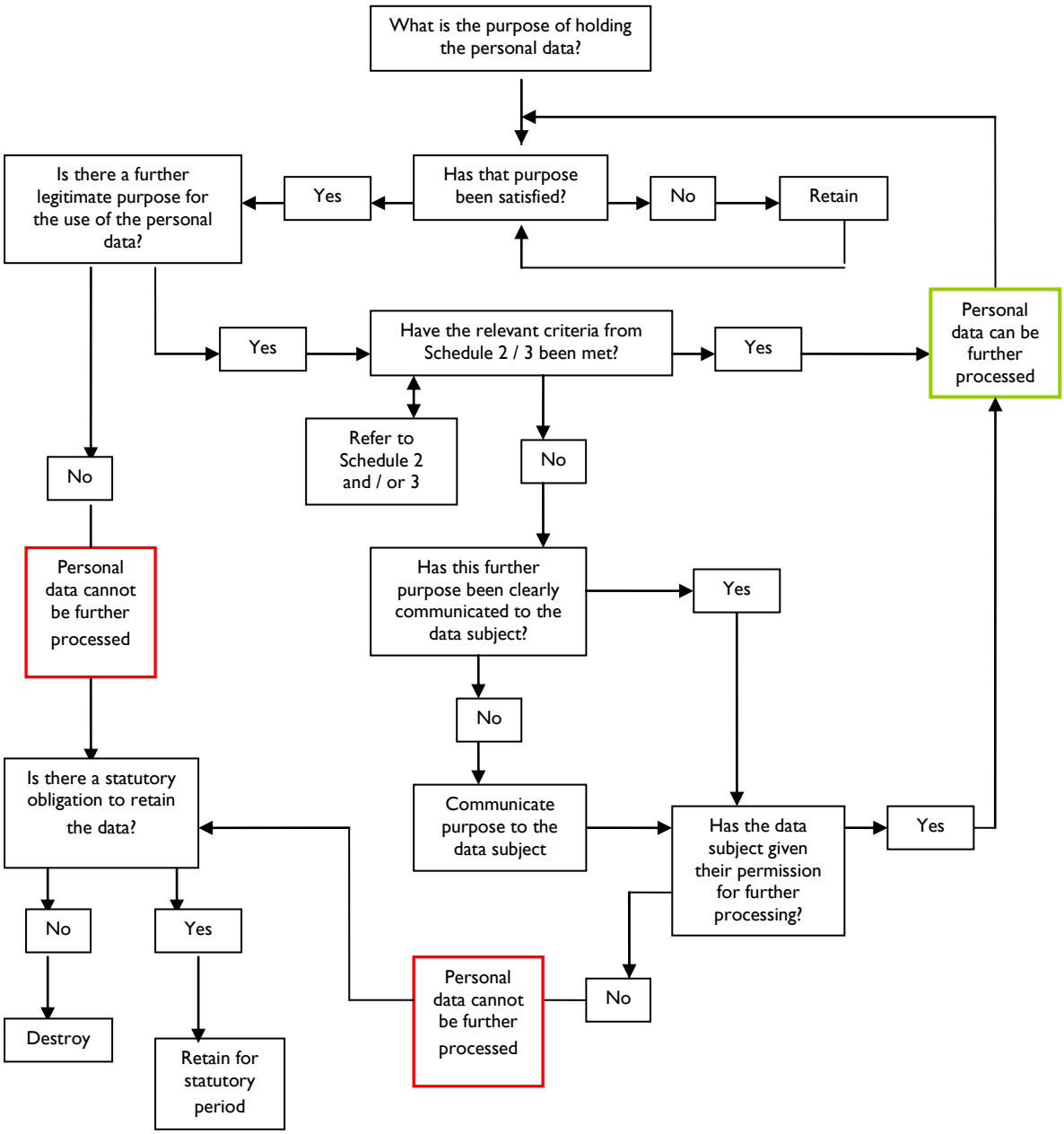
Assuming that the reason for collecting personal data from a data subject has been clearly communicated to them in an explicit statement on a form, the Library now holds that person's data to use for the purpose that the data subject consented to. Now, imagine that the Library wants to use that personal data for another purpose, or wants to process it in a way that is

different to the manner of processing that the data subject originally consented to: is it allowed to do this?

The answer is **yes**, so long as the Library can communicate to the data subject the legitimate purpose or further processing, and as long as it can satisfy Schedule 2 (or Schedule 3 with regard to sensitive personal data) of the Act. The answer is **no** if it cannot fulfil these requirements.

If a data subject has given their consent to particular data processing based on a justifiable understanding of what they have consented to, it would not be fair processing (and therefore not compliant with the first principle) to assume that they are aware of internal data processing procedures that have not been communicated to them. The clearer the data capture statement, the less likely it is that this predicament will arise.

The following flowchart shows the process that must be taken in order to ensure that data processing complies with the first, second, and fifth principles.


What is the purpose of holding the personal data?
Has that purpose been satisfied?
Yes
Is there a further legitimate purpose for the use of the personal data?
No
Retain
Yes
Have the relevant criteria from Schedule 2 / 3 been met?
Yes
Personal data can be further processed
Refer to Schedule 2 and / or 3
No
No
Personal data cannot be further processed
Has this further purpose been clearly communicated to the data subject?
Yes
No
Is there a statutory obligation to retain the data?
Communicate purpose to the data subject
Has the data subject given their permission for further processing?
Yes
No
Yes
Personal data cannot be further processed
No
Destroy
Retain for statutory period

APPENDIX VI – Third party personal data in the Library collections

In addition to the personal data that the Library holds within its business information, the Library also holds personal data within its collections. Books (think of biographies) are rich in personal data. However, it is safe to assume that in the publishing of a book, the publisher takes on board the risks associated with processing personal data, such as libel and defamation issues. Nevertheless, we ask all readers to observe the Library's code of practice which states "Readers should ensure that any information obtained from our collections relating to living individuals is used in accordance with the principles of the Data Protection Act 1998".

Manuscript and moving image collections, however, need further consideration. Imagine that you write letters to a friend, imparting all manner of personal detail about your life. Imagine that your friend becomes famous. Imagine that your friend sells their collection of letters to the National Library of Scotland. Your life is now laid bare to the public without your consent. This issue of third party data in the Library's collections is a challenging one.

The Act states, under section 33, that personal data is exempt for the purposes of research. However, any such processing of personal data may only take place under certain conditions. These are:

1. that the data is not processed to support measures or decisions with respect to particular individuals, and
2. that the data is not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject, and
3. that the results of the research or any resulting statistics are not made available in a form which identifies data subjects.

The retention of personal data for research purposes only, and the further processing of it, does not violate the second and fifth data protection principles.

The situation regarding third party data in manuscripts collections has been explored in more detail. This was as a result of a member of the public objecting to their personal letters appearing in one of the Library's collections that another person had sold to the Library. The objection was on the grounds that disclosing his personal data would cause substantial damage and distress. The Library submitted a case to the Information Commissioner who in turn discussed the matter with their legal department. The final decision was that the member of the public should be able to block access to the aspects of the collection that are his personal data.

This has huge implications for manuscript and moving image collections and challenges the current understanding of section 33 of the Data Protection Act. One logical conclusion based on the Commissioner's decision is that all third party data subjects who are identifiable and alive should be able to block processing in order to prevent substantial damage and distress, although this remains a topic of much debate. The status of category (e) data is such that data subjects' rights are restricted with regard to the ability to prevent

processing. Much of the third party data would classify as category (e). However, in the particular instance above, the data subject was able to identify exactly where the sensitive personal data was and it would not have been appropriate to class their data as category (e).

Staff should remember that the Act only applies to identifiable living individuals. There is no expectation that staff should check through every manuscript or moving image collection and ascertain whether individuals are still alive or not. The guidance from the Society of Archivists advises that a life expectancy of 100 years is assumed. This means that the conditions for use of personal data for research purposes need only apply to material that is likely to contain the personal details of people born in (at the time of this document) 1914 or after.

It is important that the Library engages with its users in this area. Doing so will provide an opportunity to explain the requirements of the law to users, and will also provide an opportunity to further guard against the risk of non-compliance with the Act. The best way to do this is by introducing a requirement for users to fill in a disclaimer. The form called “Permission to consult material which may contain personal data as defined by the Data Protection Act 1998” should be used. Readers are required to fill one in whenever they consult material that falls within the 100 year period. It is also good practice to recommend to researchers to anonymise their research whenever it is possible.

If the Library acquires a collection that features sensitive personal data relating to identifiable living individuals, the Library should apply restrictions on the use of the collection, such as an embargo, until such time as the personal data is no longer sensitive in its nature.

In addition to the above considerations, the Library must also establish how to deal with third party personal data that it holds when it is not the data controller, for example when manuscripts collections are on deposit, or when staff hold the data of other organisations. These matters will be considered in the next section.

APPENDIX VII – Personal data that the Library doesn't "own"

It is important in any data protection scenario to understand who the data controller is. The data controller is defined as a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

It should be assumed that when the Library "owns" its data, the Library is the data controller with respect to this data. The vast majority of data held by the Library belongs to the Library. However, there are instances where personal data is on Library premises, but that data does not belong to the Library.

The main area where this occurs is in deposited collections. Best practice in this area is demonstrated by the "Form of agreements over deposits" in use by the Division of Manuscripts. Clause 13 of the agreement establishes that the Library accepts deposits on the understanding that the Depositor remains the data controller. The terms of the deposit agreement will typically govern the use of the collection, and in the agreement it is established that the Library will act as data processor on behalf of the data controller. During deposit negotiations, the Library should discuss this issue fully with the data controller. In the event of sensitive data issues arising, the Library may wish to consider whether it would be happy to process this data, and may write more precise conditions into the Deposit Agreement that would protect the Library from any legal damages action. Notwithstanding the identity of the data controller, the guidance about the use of third party data given in the previous section should still be applied when Library users are using collections affected by the 100 year rule for research purposes.

The Library may also find that it has personal data on its premises which does not "belong" to the Library, but rather, "belongs" to an individual member of staff. Many staff are members of outside professional groups or organisations, and some of these staff may hold posts in these groups or organisations that involve the holding of personal data. In these instances, the Library is not the data controller, nor is the corporate body performing the role of a data processor. Any staff that are holding this kind of data should keep it separate from the Library's corporate information and held securely. They are also advised to make themselves aware of who the data controller is with regard to the information they hold, and to ensure that they are compliant with the requirements of the DPA.

The last category exists where the Library is involved in some sort of partnership, consortium, or other such arrangement, and where as a result of that arrangement, personal data is processed. The joint parties must agree upon the determination of the purposes for which personal data is acquired, and the manner in which personal data will be processed. The joint parties will be the data controller for this personal data. The duties of joint data controllers are just as those for individual data controllers and any joint agreements must be compatible with the Library's Data Protection Policy.

APPENDIX VIII – Holding of publishers' details

The Library holds many details of publishers. The name and address of a firm is not classified as personal data, because it is not data about an individual. However, there is some concern about sole traders, or self publishers, where the name and address of the "company" is likely to be the name and / or address of an individual. This matter is made more pressing when we consider that small or self publishers are sometimes publishing material that other publishers did not want to publish, perhaps because of controversial subject matter. The name and address of a self publisher of pamphlets about abortion, religion, politics, drugs, and so on, may actually be considered as sensitive personal data.

Furthermore, this isn't idle data. There is a legitimate interest in wanting to know the name and address of a publisher because of the Copyright Designs and Patents Act. If a reader wishes to copy more than the fair dealing arrangements permit, then they can contact the publisher and request permission. But they can only do this if they know who to contact.

In the event that the publisher's contact details are not contained in the publication, or that the contact details cannot be retrieved from the public domain (such as a website or telephone directory), then it is typical for the user to ask the Library for the contact details.

Current practice at the Library appears to be best practice in this area: the Library liaises between user and publisher, satisfying the CDPA without risking a breach of the DPA. For clarification, staff must not give out the personal data of data subjects to other people without the consent of the data subject. In the instance of a publisher who is only known by their own name, or when it is unclear whether the publisher is an individual or a firm, the Library should assume that the publisher is an individual. When there are no publishers' details available to Library staff either, it follows that there is no personal data to act upon.

It is important that publishers are aware that we are processing their data, and the manner in which their data is held and processed should be communicated to them. Condition 3 in Schedule 2 indicates that the Library does not need to seek consent to process this data, so the communication of purpose and processing could be issued with the letter of receipt to the publisher (this assumes therefore that the publisher has supplied a contact address). The following statement should be included in correspondence with publishers:

"The Library holds records of publisher details in order to keep track of legal deposit claims and receipts. Access to the database is restricted to members of staff involved in acquisition and processing of legal deposit material. Staff in these areas may contact you with regard to the Library's obligations under the Copyright, Designs and Patents Act 1988. Please notify the Library of any

change to your details. All personal data held by the Library will be processed in accordance with the Data Protection Act 1998".

A different statement could be prepared if there was a legitimate reason for other users to have access to the database. Publishers could even be asked if they would like to opt in to an open register of publishers. However, any such reworking would make consent necessary, whereas the current statement is mainly to inform data subjects about the Library's obligations under the CPDA and the Legal Deposit Act.

The eighth data protection principle states that 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. For this reason, the names and addresses of publishers (which may contain direct reference to identifiable living individuals) should not be stored in a system that may transmit this data outside the European Economic Area, for example, a system such as Voyager.

APPENDIX IX – Names of donors in fundraising campaigns

One of the more difficult personal data issues to tackle involves the treatment of the personal data belonging to prospective donors. Before a person can be approached regarding fundraising, and therefore before they can consent to their personal data being processed for this purpose, an amount of personal data must be processed beforehand.

The guidance from the Institute of Fundraising reflects the best practice in this area. They suggest that, providing all principles of data collecting are being followed, it is appropriate to seek consent for data processing at the first formal contact. This contact should explain the purposes and the manner in which their personal data will be processed, and should allow the data subject to opt out of the campaign. The personal data belonging to prospects that ask to be removed from data processing should be destroyed immediately and only their identity recorded in the campaign database to ensure that they are not contacted again.

Once data subjects have consented to their data being processed, the data processing regulations apply accordingly. Given the nature of the data purpose, it is likely that sensitive personal data may form part of the dataset. Typically, the ability to process sensitive personal data depends on receiving the explicit consent of the data subject. However, condition 5 of Schedule 3 allows sensitive personal data to be processed without consent when "the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject". It is important that staff undertaking this sort of data processing establish whether such information was deliberately made public by the data subject, as opposed to being exposed by journalists, for example.

Financial data should be retained in accordance with the regulations governing financial data. It will also be necessary to retain the personal data of any donors or non-donors who have registered an interest in participating in ongoing fundraising campaigns. However, when prospects opt out of the fundraising process, or when donors commit only to a particular fundraising campaign, their personal details should only be kept for as long as they serve the purpose for which they were acquired. Skeleton details should be retained so that these data subjects are not contacted again having registered their choice not to be contacted for fundraising purposes (and similarly so for direct marketing campaigns).