THE INSTITUTE OF MASTERS OF WINE

DATA PROTECTION POLICY

Bates Wells Braithwaite London
2-6 Cannon Street
London EC4M 6YH
Tel: 020 7551 7777
Ref: MOR/212021/0010

Contents

1. Purpose of the policy

1.1 The Institute of Masters of Wine ("**the Institute**") is committed to complying with privacy and data protection laws including the Data Protection Act 1998 (**"the DPA"**). This policy sets out the principles we will apply when handling individuals' personal information.

1.2 The Institute must comply with the DPA and this policy. It is the responsibility of any staff member who handles or processes personal data to ensure that we comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action.

1.3 A failure to comply with this policy could expose the Institute to enforcement action by the Information Commissioners Office (**"the ICO"**). The ICO has powers to issue notices requiring compliance with the DPA, to require organisations to co-operate with its enquiries, to search and seize material and to issue substantial fines. This could ultimately result in restrictions being imposed on our use of some or all of our databases or in complaints or claims for compensation from affected individuals.

1.4 This policy may be amended from time to time to reflect any changes in legislation or internal policy decisions.

2. About this policy

2.1 The types of personal information that we may handle include details of:

- current, past and prospective employees;
- current, past and prospective students;
- Masters of Wine;
- individual contractors and suppliers; and
- anyone else we communicate with or whose personal data we collect.

2.2 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.3 The Data Protection Compliance Manager is responsible for ensuring compliance with the DPA and with this policy. That post is held by the Programme and Development Manager, Oliver Chapman, 020 7383 9130, ochapman@mastersofwine.org. Any questions or concerns about this policy should be referred in the first instance to the Data Protection Compliance Manager.

2.4 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or the Data Protection Compliance Manager.

3. Definitions of data protection terms

The following terms will be used in this policy and are defined below:

3.1. **Data subjects** include all living individuals about whom we hold personal data, for instance an employee or student of the Institute. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.2. **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.3. **Data controllers** are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to process personal data in line with the DPA. The Institute is the data controller of all personal data that we manage as part of our business

3.4. **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include third parties such as website hosts which handle personal data on our behalf.

3.5. **European Economic Area** includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.6. **ICO** means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

3.7. **Processing** is any activity that involves use of personal data. It includes obtaining, recording, holding, organising, amending, retrieving, using, disclosing, erasing or destroying data.

3.8. **Sensitive personal data** includes information about a person's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life or orientation; or
- commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

4. Data protection principles

4.1 Anyone processing personal data must comply with the eight enforceable data protection principles. The Institute is required to comply with these principles (summarised below) in respect of any personal data which it deals with as a data controller.

Personal data should be:

4.1.1 processed fairly and lawfully;

4.1.2 processed for the purposes which have been specified to the individual data subject, and not in any way incompatible with those purposes;

4.1.3 adequate, relevant and not excessive for the purpose;

4.1.4 accurate and, where necessary, kept up to date;

4.1.5 not kept longer than necessary for the purpose;

4.1.6 processed in line with data subjects' rights;

4.1.7 secure; and

4.1.8 not transferred to people or organisations outside the European Economic Area without adequate safeguards.

5. Processing data fairly and lawfully

5.1 The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes communicated to the data subject.

5.2 To do this, every time the Institute receives personal data, which we intend to keep (e.g. information about individual students) it is necessary to give the subjects of that data **"the fair processing information"**. In other words information about:

5.2.1 who will be holding their information, i.e. the Institute;

5.2.2 why the Institute is collecting their information and what we intend to do with it; and

5.2.3 anything else necessary to make sure that the Institute is using their information fairly, for example, if we plan to pass this information to another organisation.

5.3 This fair processing information can be provided on web pages, in mailings or on application forms. It is currently provided to students in Clause 16 of the latest version of the Learning Agreement.

6. Processing data for the original purpose

6.1 The second data protection principle requires that personal data only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the DPA.

6.2 This means that personal data should not be collected by the Institute for one purpose and then used for another. If it becomes necessary to change the purpose for which the

data is processed, the data subject should be informed of the new purpose before any processing occurs, for example, if we collect personal data, such as a contact number or email address, for the purpose of communicating with a Master of Wine it should not then be used for any new purpose, for example passing those details to other organisations for marketing purposes, without the consent of the individual.

7. Personal data should be accurate

The third and fourth data protection principles require that personal data kept by the Institute should be accurate, adequate and relevant. Information which is incorrect or misleading is not accurate and therefore staff are required to check the accuracy of any personal data held by the organisation, e.g. information relating to members, at the point of collection and [at least once annually] after that point. Inaccurate or out-of-date data should be destroyed.

8. Not retaining data longer than necessary

8.1 It is a requirement of the fifth data protection principle that personal data should not be kept longer than is necessary for the purpose it was collected for. This means that the personal data that the Institute has collected should be destroyed or erased from our systems when it is no longer required.

8.2 For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please contact the Data Protection Compliance Manager.

9. Rights of individuals under the DPA

9.1 The DPA gives people rights in relation to how organisations process their personal information. Staff members need to be aware of these rights. They include (but are not limited to) the right:

9.1.1 to request a copy of any personal data held about them by the Institute (as data controller), plus a description of the type of information being processed, the uses that are being made of the information and details of anyone to whom their personal data has been disclosed (this is known as the right of subject access);

9.1.2 to have to have inaccurate data amended or destroyed; and

9.1.3 to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

10. Data security

10.1 The seventh data protection principle requires that data be kept secure.

10.2 The Institute is required to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

10.3 If the personal data is sensitive, an additional level of security should be applied, for instance, if sensitive personal data (such as details of the health of staff members) is held on a memory stick or other portable device you should always encrypt it because the potential reputational and other damage to the Institute is likely to be greater if the information is lost or stolen.

10.4 When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

10.5 The following security procedures must be followed in relation to all personal data processed by the Institute:

10.5.1 **Entry controls:** Any stranger seen in entry-controlled areas should be reported;

10.5.2 **Equipment:** Staff should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended;

10.5.3 **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind, including physical copies of students' exam results. (Personal information is always considered confidential);

10.5.4 **Methods of disposal:** Paper documents should be shredded. Memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required;

10.5.5 **User access controls:** Access to personal data on the Institute's database should be controlled:

- all computers should be password protected;
- all staff should have their own individual password which should be shared only on a need to know basis;
- computers should have password activated screen savers that can be turned on whenever the user is away from his or her desk;
- passwords should include a mixture of letters and numbers, avoid passwords that are easy to guess such as an employee's name or date of birth;
- staff access to the database should restricted. Different rights of access should be allocated to different users depending on job description and their need to access personal or confidential data.

10.5.6 **Backing up data:** Daily back-ups should be taken of all data on the Institute's system; data should not be stored on local drives or removable media as these will not be backed up;

10.5.7 **Travelling with personal data and remote working:** Staff must keep data secure when travelling or using it outside of the Institute's offices. For instance:

- documents and laptops must be kept secure (not left lying around off site);
- data stored on computers when working at home must be password protected, and kept confidential;
- when you are working from home, you should ensure that the laptop or computer you are using is securely protected from theft while you are away from it.

10.5.8 **Secure exchange of data:** Data must always be transferred in a secure manner. The degree of security required will depend on the nature of the data; the more sensitive and confidential the data, the more stringent the security measures should be. The following precautions should be taken:

- use registered post or courier. Never send a CD or stick containing personal data by normal post;
- use password protection (on files) if sending by email – but recognise this is not very secure and should only be used for small quantities of information;
- never send sensitive data, by email unless it has been encrypted (speak to the Head of IT for more details).

11. Transferring Data Outside the EEA

11.1 The eighth data protection principle requires that when where organisations transfer personal data outside the EEA they take steps to ensure that the data is properly protected. The Institute has staff members in Australia with whom it is sometimes necessary to share personal data relating to students and others.

11.2 The European Commission has determined that New Zealand provides adequate protection for the rights and freedoms of data subjects. As such personal data may be transferred there without any further restrictions than those listed in the rest of this policy. In transferring personal data to Australia or other countries outside the EEA, it may be necessary to seek the consent of the individuals whose data is being transferred or to enter into an EC-approved agreement.

11.3 For more information, please speak to the Data Compliance Manager.

12. Processing sensitive personal data

12.1 On some occasions the Institute may collect information about our students and other individuals that is defined by the DPA as sensitive, and special rules will apply to the processing of it. The categories of sensitive data are set out in the definitions in section 3.

12.2 Purely financial information is not technically defined as sensitive personal data by the DPA, however, particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously.

12.3 In most cases, in order to process sensitive personal data, the Institute must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information.

12.4 It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the DPA permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please speak to the Data Protection Compliance Manager.

13. Paper files

13.1 Most paper records (i.e. data not held on a computer system) technically are not covered by the DPA. The only paper records which are subject to the DPA are those which are held in a highly ordered filing system, for example certain HR records.

13.2 However, to follow best practice, the Institute should treat paper records as though the DPA applies to them, following the procedures set out in this policy.

14 Notification

14.1 The organisation's data protection notification defines our data subjects (i.e. the people about whom we hold personal data), our data categories (the information we hold about them) and our purposes (the reasons why we hold this information). A copy of our notification may be viewed on request, or online via the public register on the web site of the ICO (www.informationcommissioner.gov.uk).

14.2 Processing which is not included in our Notification (additional purposes or types of information) should not take place. The Notification is reviewed once a year to ensure it is still accurate and up to date. If you think we are, or should be, processing data that is not covered by our Notification, please tell the Data Protection Compliance Officer immediately.

15 Monitoring and review of the policy

15.1 This policy is reviewed yearly by our Council to ensure that it is achieving its stated objectives.

Appendix

MODEL DATA PROCESSING AGREEMENT

DRAFTING NOTES

PLEASE READ BEFORE USING THE MODEL AGREEMENT

Read and follow the guidance carefully and replace the italicised wording in the agreement with the appropriate information. Before giving the model agreement to a data processor, make sure that you delete any square brackets and footnotes.

When do I use this model agreement?

1. This agreement can be used whenever another organisation is processing personal data on behalf of the Institute of Masters of Wine ("**the Institute**"). *Personal data* will include almost any information about individuals, which could be used to identify them, for instance, names and addresses of students of the Institute, Masters of Wine or information about employees of the Institute. The other organisation could be a software provider, payroll function provider or any organisation carrying out services for the Institute involving the use of individuals' personal information, e.g. IT or other services. Alternatively, the organisation could be processing data on behalf of the Institute on a one-off basis, for instance to test software on the Institute's behalf.

2. The Data Protection Act 1998 requires all data controllers to take appropriate technical and organisational measures to protect the personal data they process, whether they process the data for themselves or another party does so on their behalf. The Institute is a data controller of personal data which it processes for its own purposes, i.e. in circumstances where it decides how and why particular personal data should be used.

3. When allowing another party to carry out processing on behalf of the Institute, you should be satisfied that the Institute has selected a reputable organisation that it considers is able to process the Institute's data in a secure manner.

4. As a data controller, the Institute must have a written contract in place with such organisations (known as a data processing agreement). The contract must:

4.1 require the data processor to implement appropriate security measures to protect the personal data it holds on the Institute's behalf and;

4.2 ensure that the data processor only processes information on the Institute's instructions.

5. The attached model agreement should be used every time personal data is shared with a data processor to ensure that these legal requirements are complied with.

Should this agreement be used any time that we share personal data with another organisation?

6. This agreement should only be used where the organisation that you are sharing personal data with will be processing the information on behalf of the Institute. If the organisation wishes to use the information for its own purposes the model agreement will not be appropriate. [If you wish to share personal information with other organisations in this context, please speak to the [***Data Protection Officer/Penny Richards***].]

What else do I need to know?

7. When developing and negotiating this agreement with a data processor, it is essential that you consider the following issues:

7.1 Always check **where** the data processor is planning to process/hold the Institute's data. If data is being processed outside the European Economic Area ("the EEA" which includes all 27 member states of the EU and Iceland, Liechtenstein and Norway) the Institute needs to ensure that adequate measures are in place to ensure that the data is properly protected. This may require the Institute to enter into a different agreement with the data processor which contains model clauses approved by the European Commission. For more information on this, please speak to [***the Data Protection Officer/Penny Richards***].

7.2 Make sure both parties understand before entering into the agreement how personal data will be transferred from the Institute or otherwise made available to the data processor and how the parties will arrange for that data to be transferred back to the Institute (or destroyed) on termination of the agreement.

7.3 Data processors must understand that they can process the personal data transferred only on the express instructions of the Institute. They cannot contact individuals for any other purpose, e.g. to send marketing materials relating to their own or any third party's services.

7.4 The Institute should monitor the data processor regularly to ensure that the security measures it has in place are appropriate and comply with Schedule 1 of the template agreement.

8. Do not delete any clauses in the attached agreement (other than optional clauses) without checking first with [***the Data Protection Officer/Penny Richards***].

9. The agreement is drafted to allow for two alternative data sharing arrangements. The first will apply where the Institute is entering into a separate service agreement with the data processor. The second is where there is a one-off sharing of data for any other reason. Alternative drafting has been included to allow you to amend the document as appropriate to reflect the background to the data sharing. The footnotes should be used to help determine which wording should be deleted or included.

DATED **20[14]**

THE INSTITUTE OF MASTERS OF WINE

and

[*INSERT NAME*[1]]

SUBJECT TO AGREEMENT

AGREEMENT WITH DATA PROCESSOR

Bates Wells Braithwaite
2–6 Cannon Street
London EC4M 6YH

1 Insert name of supplier/organisation that will be processing personal data on behalf of the Institute and acting as a data processor.

Agreement

Dated: 20[14]

Parties:

(1) **THE INSTITUTE OF MASTERS OF WINE**, a company limited by guarantee and registered in England and Wales (registration no. 1059707) with registered office at 24 Fitzroy Square, London, W1T 6EP

(the "**Data Controller**")

and

(2) ***[INSERT DETAILS OF DATA PROCESSOR[2]]***

(the "**Data Processor**")

Background

(A) The Data Controller

Option 1 [uses the services of the Data Processor from time to time to [*insert activity e.g. carry out marketing/data cleaning services/provide payroll services]*.] ***OR***

Option 2 [has agreed to share personal data in relation to which it is a data controller with the Data Processor so that the Data Processor can *[insert details of why data is being shared with Data Processor if this is not in connection with a service agreement, e.g. so that the Data Processor can test software on behalf of the Data Controller]*]**.**

(B) The Parties have agreed to enter into this Agreement to ensure compliance with the Data Protection Act 1998 in relation to all such processing.

Interpretation

The terms and expressions set out in this agreement shall have the following meanings:

"Act" means the Data Protection Act 1998;

["Contract" the [service] agreement between the parties dated [*insert date]*;][3]

"Data Controller", "Data Processor" and "processing" shall have the meanings ascribed to them in the Act;

"ICO" means the Information Commissioner's Office;

---

2 Insert full name, registered address and company number (if applicable) of data processor.

3 Only insert this definition if the Institute is also entering into a separate service agreement with the data processor.

"personal data" shall include all data relating to individuals which is processed by the Data Processor on behalf of the Data Controller in accordance with this Agreement.

It is agreed as follows:

1. The terms of this Agreement are to apply to all data processing carried out for the Data Controller by the Data Processor and to all personal data held by the Data Processor in relation to all such processing whether such personal data is held at the date of this Agreement or received afterwards.

2. **Option 1:** [This Agreement sets out various obligations in relation to the processing of personal data under the Contract by the Data Processor. If there is a conflict between the provisions of the Contract and this Agreement, the provisions of this Agreement shall prevail.]

   Option 2: [This Agreement sets out various obligations in relation to the processing of personal data in connection with [*insert description of why Data Processor is processing data for the Data Controller*]. The terms of this Agreement shall supersede any previous arrangement, understanding or agreement between the parties relating to data protection.]

3. The Data Processor is to [carry out [*describe services as in (A) above]*/ [*insert brief description of other reason why Data Processor is processing personal data on behalf of the Institute, if not as part of a service agreement]* and will process personal data only on the express instructions of designated contacts at the Data Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Data Controller to the Data Processor [*during the term of the Contract*]/[*at any time*][4]).

4. The Data Processor shall comply at all times with the Act and shall not perform its obligations under this Agreement [*or the Contract*][5] in such way as to cause the Data Controller to breach any of its applicable obligations under the Act.

5. All personal data provided to the Data Processor by the Data Controller or obtained by the Data Processor in the course of its work with the Data Controller is strictly confidential and may not be copied, disclosed or processed in any way without the express authority of the Data Controller.

6. The Data Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with all applicable legislation from time to time in force and any best practice guidance issued by the ICO.

7. Where the Data Processor processes personal data (whether stored in the form of physical or electronic records) on behalf of the Data Controller it shall:

---

4 Delete as appropriate depending on whether the Institute is entering into a separate agreement with the data processor.

5 As in footnote 4 above.

7.1 process the personal data only to the extent, and in such manner, as is necessary in order to comply with its obligations [*under the Contract*]/[*to the Data Controller*[6]] or as is required by law or any regulatory body including but not limited to the ICO;

7.2 implement appropriate technical and organisational measures and take all steps necessary to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested from the Data Controller;

7.3 in furtherance of its obligations under 7.2 above implement and maintain the security measures set out in Schedule 1 to this agreement;

7.4 if so requested by the Data Controller (and within the timescales required by the Data Controller) supply details of the technical and organisational systems in place to safeguard the security of the personal data held and to prevent unauthorised access;

7.5 on reasonable prior notice, permit persons authorised by the Data Controller to enter into any premises on which personal data provided by the Data Controller to the Data Processor is processed and to inspect the Data Processor's systems to ensure that sufficient security measures are in place;

7.6 notify the Data Controller (within two working days) if it receives:

7.6.1 a request from a data subject to have access to that person's personal data; or

7.6.2 a complaint or request relating to the Data Controller's obligations under the Act.

7.7 provide the Data Controller with full co-operation and assistance in relation to any complaint or request made in accordance with clause 7.6.

7.8 not process personal data outside the European Economic Area without the prior written consent of the Data Controller [and, where the Data Controller consents to a transfer, to comply with the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Act by providing an adequate level of protection to any personal data that is transferred];

7.9 not transfer any personal data provided to it by the Data Controller to any third party without the written consent of the Data Controller and ensure that any third party to which it sub-contracts any processing has entered into a written contract with the Data Processor which contains all the obligations that are contained in this Agreement and which permits both the Data Processor and the Data Controller to enforce those obligations.

8. The Data Processor shall transfer all personal data to the Data Controller on the Data Controller's request in the formats, at the times and in compliance with the specifications set out in Schedule 2.

---

6 Delete as appropriate depending on whether the Institute is entering into a separate agreement with the data processor.

9. The Data Processor shall be liable for and shall indemnify (and keep indemnified) the Data Controller against each and every action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and disbursements on a solicitor and client basis) and demand incurred by the Data Controller which arise directly or in connection with the Data Processor's data processing activities under this Agreement, including without limitation those arising out of any third party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with any part of this Agreement by the Data Processor of its employees, servants agents or sub-contractors.

10. The Data Processor agrees that in the event that it is notified by the Data Controller that it is not required to provide any further services to the Data Controller under this Agreement, the Data Processor shall transfer a copy of all information (including personal data) held by it in relation to this Agreement to the Data Controller in a format chosen by the Data Controller and/or, at the Data Controller's request, destroy all such information using a secure method which ensures that it cannot be accessed by any third party and shall issue the Data Controller with a written confirmation of secure disposal.

11. All copyright, database rights and other intellectual property rights in any personal data processed under this Agreement (including but not limited to any updates, amendments or adaptations to the personal data by either the Data Controller or the Data Processor) shall belong to the Data Controller. The Data Processor is licensed to use such data only for the term of and in accordance with this Agreement.

12. **Option 1:** [*The Data Processor accepts the obligations in this Agreement in consideration of the Data Controller continuing to use its services*][7].

    or

    Option 2: [*The Data Processor accepts the obligations in this Agreement in consideration of the payment of £1 from the Data Controller which the Data Processor hereby acknowledges.]*

13. The Data Processor agrees that from time to time the Data Controller may update this Agreement to reflect changes in data protection law or the data sharing arrangements between the parties.

14. This Agreement shall be governed by the laws of England and Wales.

[7] Use option 1 if the Institute is entering into a separate service agreement with the Data Processor. If there is no separate service agreement, option 2 should be used to ensure that there is some consideration under the contract.

SIGNED for and on behalf of
THE INSTITUTE OF MASTERS OF WINE
by:

Print Name: …….

Position: ……..

Signature: ……

SIGNED for and on behalf of
[***insert name of entity with which personal data is being shared***]
by:

Print Name: ……..

Position: ……

Signature: ……

Schedule 1
Security Measures to be adopted by the Data Processor

1. The Data Processor will ensure that in respect of all personal data it receives from or processes on behalf of the Data Controller it maintains security measures to a standard appropriate to:

1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage or destruction of the personal data;

1.2 the nature of the personal data.

2. In particular the Data Processor shall:

2.1 have in place and comply with a security policy which:

2.1.1 defines security needs based on a risk assessment;

2.1.2 allocates responsibility for implementing the policy to a specific individual or members of staff;

2.1.3 is provided to the Data Controller on or before the commencement of this Agreement;

2.1.4 is disseminated to all relevant staff; and

2.1.5 provides a mechanism for feedback and review.

2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the personal data in accordance with best industry practice;

2.3 prevent unauthorised access to the personal data;

2.4 ensure its storage of personal data conforms with best industry practice such that the media on which personal data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to personal data is strictly monitored and controlled;

2.5 have secure methods in place for the transfer of personal data whether in physical form (couriers rather than post should be used) or electronic form (all portable media should be encrypted);

2.6 put password protection on computer systems on which personal data is stored and ensure that only authorised personnel are given details of the password;

2.7 take reasonable steps to ensure the reliability of any employees or other individuals who have access to the personal data;

2.8 ensure that any employees or other individuals required to access the personal data are informed of the confidential nature of the personal data and comply with the obligations set out in this Agreement;

2.9 ensure that none of the employees or other individuals who have access to the personal data publish, disclose or divulge any of the personal data to any third party unless directed in writing to do so by the Data Controller;

2.10 have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of personal data) including:

2.10.1 the ability to identify which individuals have worked with specific personal data;

2.10.2 having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the Act; and

2.10.3 notifying the Data Controller as soon as any such security breach occurs.

2.11 have a secure procedure for backing up and storing back-ups separately from originals;

2.12 have a secure method of disposal unwanted personal data including for back-ups, disks, print outs and redundant equipment.[8]

[8] You may wish to impose additional security obligations on any data processor under this agreement. If you do, these should be added to this schedule.

Schedule 2

Insert details relating to the transfer of data by the Data Processor to the Institute as set out in paragraph 8 of the Agreement, including:

- content of data to be transferred;
- format of the data; and
- timings for transfers.